Oracle® Enterprise Session Border Controller

Maintenance Release Guide
Release E-C[XZ]6.4.0
Formerly Net-Net Enterprise Session Director

September 2015

ORACLE

Notices

Contents

About this guide

This Oracle Enterprise Session Border Controller Maintenance Guide supports release E-C[xz]6.4.0. It provides an overview of features and functions new in releases E-C[xz]6.4.0 M1, E-C[xz]6.4.0 M2, E-C[xz]6.4.0 M3, E-C[xz]6.4.0 M4, and E-C[xz]6.4.0 M5. This guide includes issues fixed since E-C[xz]6.4.0 GA, as well as known issues and limitations in this M5 release.

The information contained in this Maintenance Release Guide pertains to Enterprise Customers, and the following Oracle platforms:

- Server Edition. Designed for distributed small to medium enterprises, runs on a certified server. Supports a maximum of 1000 concurrent SIP audio calls.
- VM Edition. Designed for distributed small to medium enterprises, runs on a generic server within a virtual environment. Supports a maximum of 250 concurrent SIP audio calls per Virtual Machine (VM). The VM Edition supports both VMware and Hyper-V virtualization software.
- Oracle Hardware Edition. Designed for medium to large enterprises, runs on Oracle the Acme Packet 3820 and the Acme Packet 4500. Supports a maximum of 16,000 concurrent SIP audio calls.

Refer to the Oracle Enterprise Session Border Controller E-C[xz]6.4.0 documentation set for more information about each platform.

Audience

This Maintenance Release Guide is for enterprise users who want to know about new features, known issues, limitations, and caveats for the E-C[xz]6.4.0 release.

Licensing

The E-C[xz]6.4.0 M5 release is an aggregation of software from various sources and organizations. These include Oracle software, third-party commercial software used under license, and publicly available software packages distributed under various open source licenses. For more information about the applicable licenses and how to obtain the source code for the open source components, click **About** on the Web GUI Help menu, enter the show about command from the ACLI, or ask your Oracle representative.

Revision History

Date	Revision Number	Description
June 14, 2013	Revision 1.00	Maintenance Release 1 for the E-C(xz)6.4.0 version of software for the Enterprise platforms: Server Edition, VM Edition, and Oracle Hardware Edition. General feature: • Transparent support of Binary Floor Control Protocol (BFCP) over UDP and TCP Web GUI features: • New Save/Activate notification enhancement • Prompt for configuration schema update • “About” link under “Help” menu. ACLI feature: • New ACLI “quit” command in configuration mode

Date	Revision Number	Description
October 18, 2013	Revision 1.20	Adds Maintenance Release 2 content. Please see the M2 chapter for new feature listings.
November 18, 2013	Revision 1.21	Adds content on Avaya SM Dual Registrations
February 27, 2014	Revision 1.22	Adds Maintenance Release 3 content. • Configuration Inventory Widget • Dynamic Access Control List • Initial Configuration Wizard • Session Manager Mapping • Traceroute Command • Web GUI Search • Web GUI Shortcut Key Commands
July 31, 2014	Revision 1.23	Adds Maintenance Release 4 content. • Widget Favorites • Show Configuration Widget • LRT List Associated Config Name Column • Expert Mode - Discard button • TCP/FIN • SRTP Re-keying • Avaya Attended Transfer
November 2014	Revision 1.24	Adds Maintenance Release 5 content. • Administrative Security ACP License • SIP hold-refer-reinvite Option
June 2015	Revision 1.25	• Adds the Media Playback with SIPREC item to Limitations.
September 2015	Revision 1.26	• Updates the note in "New Home Page in Web GUI" to clarify that the default widgets are also subject to the SIP configuration requirement for dashboard widget displays.

1

E-C[xz]6.4.0 M1

Platforms Supported

Release E-C[xz]6.4.0 M1 runs on the following platforms:

- Oracle Hardware: Acme Packet 3820, Acme Packet 4500
- Server Edition (SE): HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition (VME): VMWare and Hyper-V

Software Images

This section describes software images for this release.

For Oracle Hardware

If you are using Oracle hardware, use the following software image: nnECx640M1.tar. The x in the file name corresponds to Oracle hardware.

The latest software is packaged in .tar format. Older releases were packaged as .xz format. When upgrading from releases previous to 6.3.9, please assure bootloader build date is 1/19/2012 or newer. You can download the most recent bootloader from the Oracle support site: support.acmepacket.com.

All Other Hardware or Software-only

If you are using hardware other than Oracle's or running this software as a VM, use the file defined in this section for your needs. The z in the file name corresponds to non-Oracle hardware or VM.

- Single system image file: nnECZ640M1.bz
- Boot Media Creator: nnECZ640M1-img-usb.exe
- Virtual Machine VMWare: nnECZ640M1-img-bin.ova
- Virtual Machine Hyper-V: nnECZ640M1-img-bin.vhd

For software-only options, the following file is pre-loaded on the USB stick for [z] builds: SWR-0028-00.tar.

Before Upgrading

Before attempting to upgrade from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, please see the Known Issues section of this 6.4.0 M1 chapter.

Browser Support

You can use any of the following Web browsers to access Oracle's Web GUI:

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle Enterprise Session Border Controller software, you should clear your browser cache before using the Oracle Enterprise Session Border Controller Web GUI.

Content Map

The following table identifies the new features in Release E-C[xz]6.4.0 M1.

Content Type	Description
Adaptation	3922 - Transparent support of Binary Floor Control Protocol (BFCP) over UDP and TCP
Adaptation	Web GUI Enhancments
Adaptation	New quit command in the ACLI

New Features

This section lists the new features available in E-C[xz]6.4.0 M1:

General feature includes:

- Transparent support of Binary Floor Control Protocol (BFCP) over UDP and TCP

Web GUI features include:

- New Save/Activate notification enhancement
- Prompt for configuration schema update
- "About" link under Help menu.

ACLI feature includes:

- New quit command in configuration mode

General Feature

The following is a new feature in Release E-C[xz]6.4.0 M1.

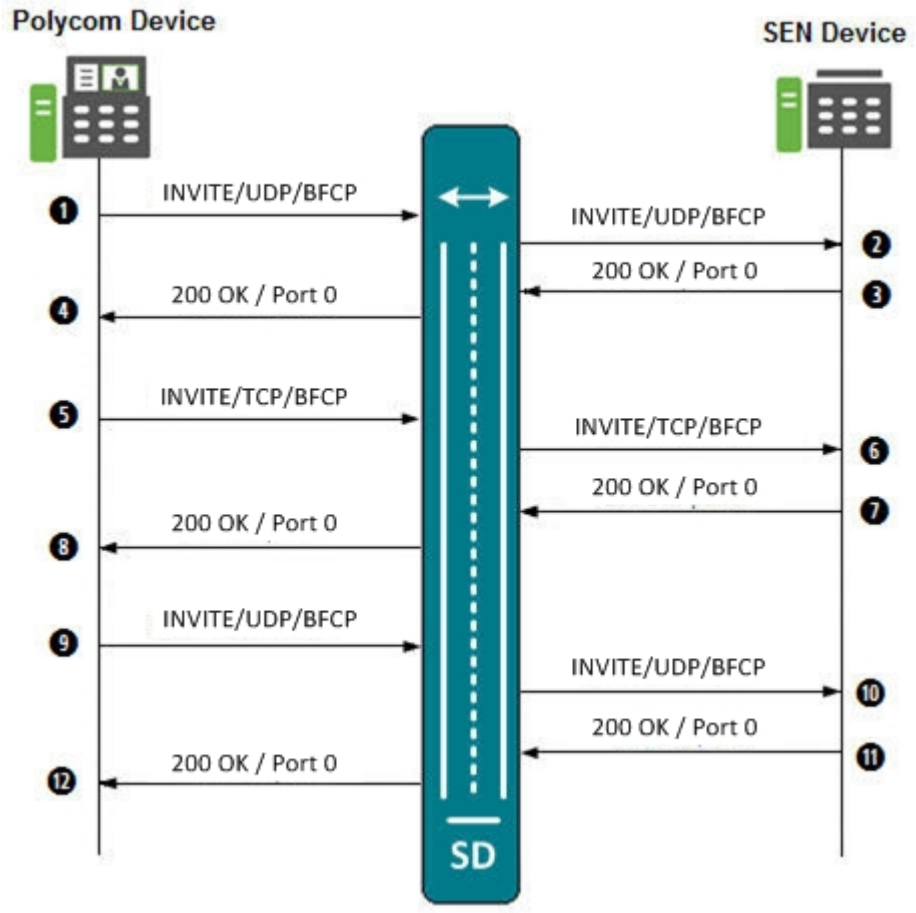
Transparent BFCP Support over UDP and TCP

Binary Floor Control Protocol (BFCP) is a protocol for controlling the access to the media resources in a conference, such as conference and media session setup, conference policy manipulation, and media control (as defined in RFC 4582).

The Oracle Enterprise Session Border Controller now supports BFCP for interworking between Polycom video devices and Siemens Enterprise Communications (SEN) endpoints. When a SIP INVITE request containing a Session Description Protocol (SDP) from a Polycom device is sent to a SEN device, the Oracle Enterprise Session Border Controller passes the INVITE request between the two devices regardless of the transfer protocol being used by the devices (UDP or TCP). It also passes the INVITE whether or not it is accepted or rejected by the destination device. The transfer protocol changes between UDP and TCP during the dialog between both endpoints on either side of the Oracle Enterprise Session Border Controller.

Note: If both endpoints on either side of the Oracle Enterprise Session Border Controller support BFCP, the BFCP is answered with the first SDP offer/answer cycle.

The following illustrates the call flow between a Polycom device and a SEN device when an INVITE is sent from the Polycom device.



The following table describes the call flow process.

Call Flow Description	
① Polycom device initiates a call to the SEN device by sending a SIP INVITE to the SD with SDP, using UDP and BFCP.	⑦ SEN device does not support BFCP, and therefore, rejects the re-INVITE, and sends a 200 Ok with port ‘0’ from the SEN side to the SD.
② SD forwards the SIP INVITE to the SEN device.	⑧ SD forwards the 200 Ok response to the Polycom device.
③ SEN device does not support BFCP, and therefore, rejects the INVITE and sends a 200 Ok with port '0' from the SEN side to the SD.	⑨ Polycom device looks at port ‘0’ and changes the media transport type from TCP to UDP. It then sends a re-INVITE to the SD.
④ SD forwards the 200 Ok response to the Polycom device.	⑩ SD forwards the re-INVITE to the SEN device.
⑤ Polycom device looks at port ‘0’ and changes the media transport type from UDP to TCP. It then sends a re-INVITE to the SD.	⑪ SEN device does not support BFCP, and therefore, rejects the re-INVITE, and sends a 200 Ok with port ‘0’ from the SEN side to the SD.

Call Flow Description	
⑥ SD forwards the re-INVITE to the SEN device.	⑫ SD forwards the 200 Ok response to the Polycom device.
	Process repeats Steps 5 through 12 until the call is accepted by the SEN device.

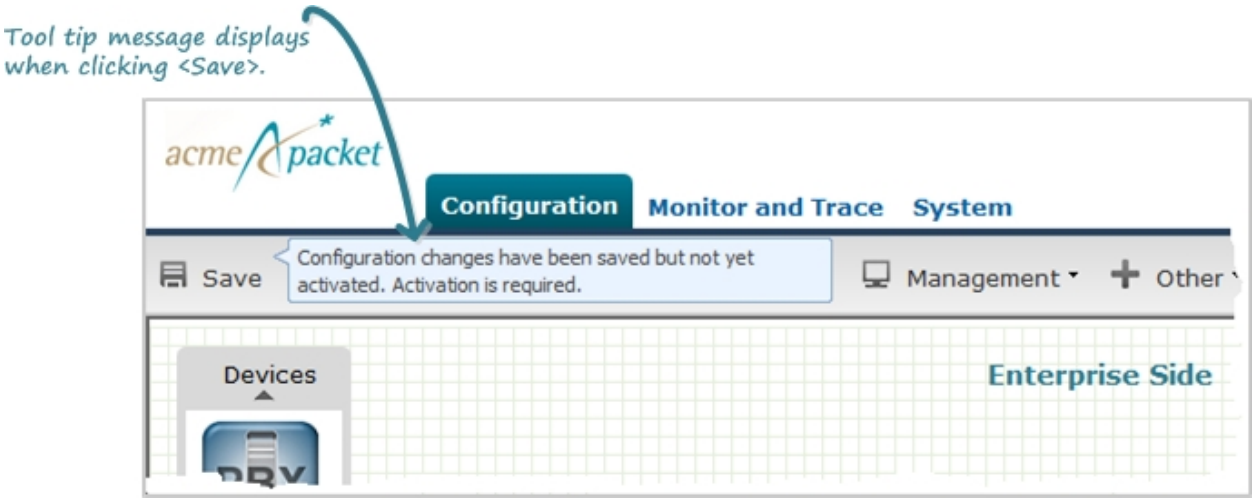
Web GUI Features

The following Web GUI features are new in Release E-C[xz]6.4.0 M1.

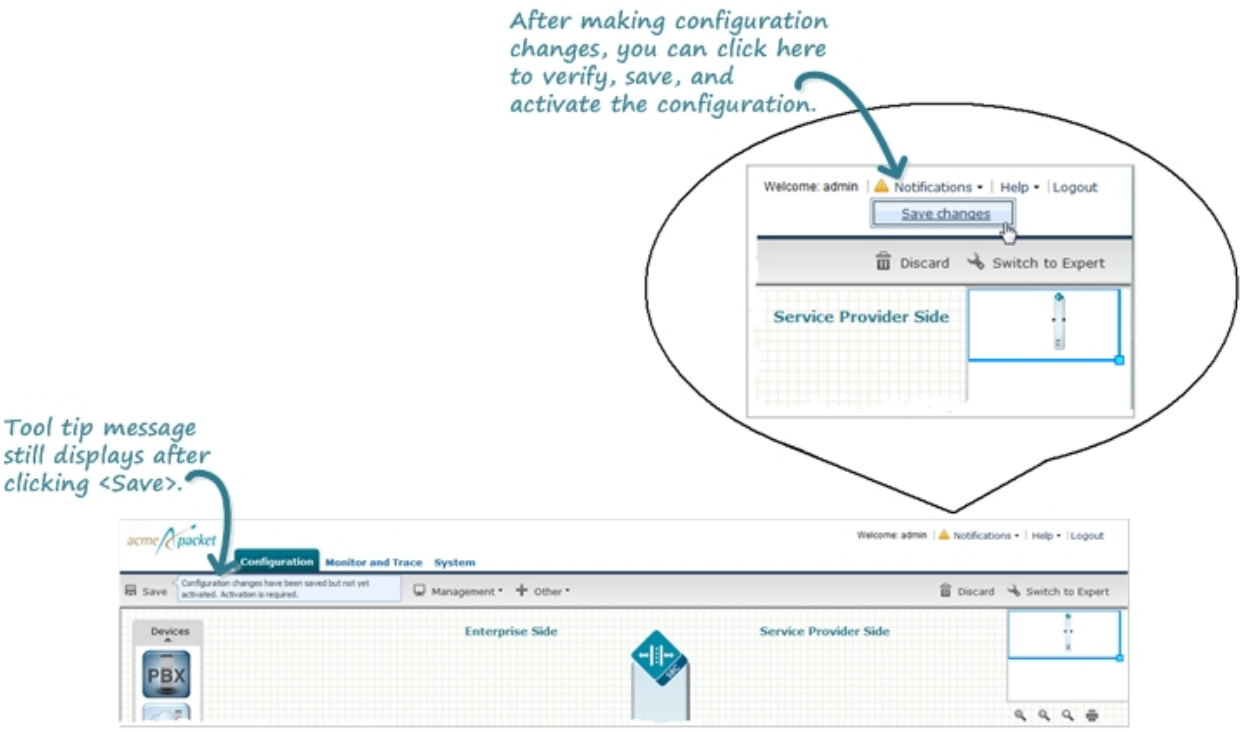
Save Activate Notification Enhancement

The Save button in the Web GUI allows you to verify and save a current configuration in both the Basic and Expert Modes. A prompt also displays giving you a choice of whether or not to activate the configuration.

Previously, after performing configuration changes and then clicking <Save>, only a tool tip message displayed as shown in the following illustration to indicate an activation was still required.



In this release after clicking <Save>, in addition to the tool tip display, a notification icon exists in the upper right corner of the screen.



This notification indicates a verify, save, and/or activate still needs to be performed on the changed configuration. You can continue to make changes to the configuration, and when you are ready to save, you can select Notifications->Save Changes, then click <Activate> at the prompt that displays.

Note: When the notification icon is grayed-out, a save and activate is not required.

Update the Configuration Schema

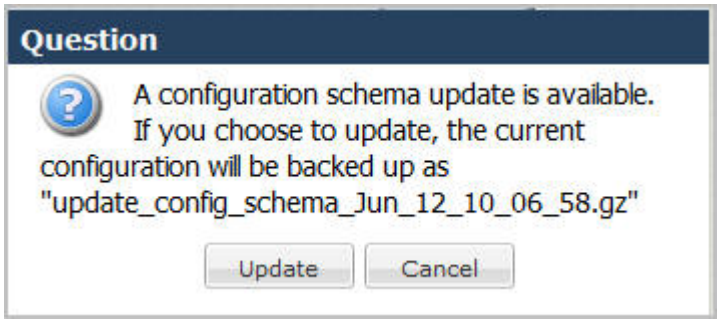
You can update the configuration parameters in your software with any new parameters included in a subsequent release by updating the schema.

Updating the schema adds any new parameters to each configuration screen in Basic Mode.

After updating your Web GUI software to a subsequent release, the system displays a schema update prompt after first log on to the GUI. If you click Cancel, the update is bypassed and no new parameters are added. The update prompt displays each time you log on to the Web GUI, until you choose to update the configuration schema.

Procedure

1. Log into the Web GUI. The system displays the following prompt.



2. Click **Update**. The system backs up the current configuration and updates the configuration schema.

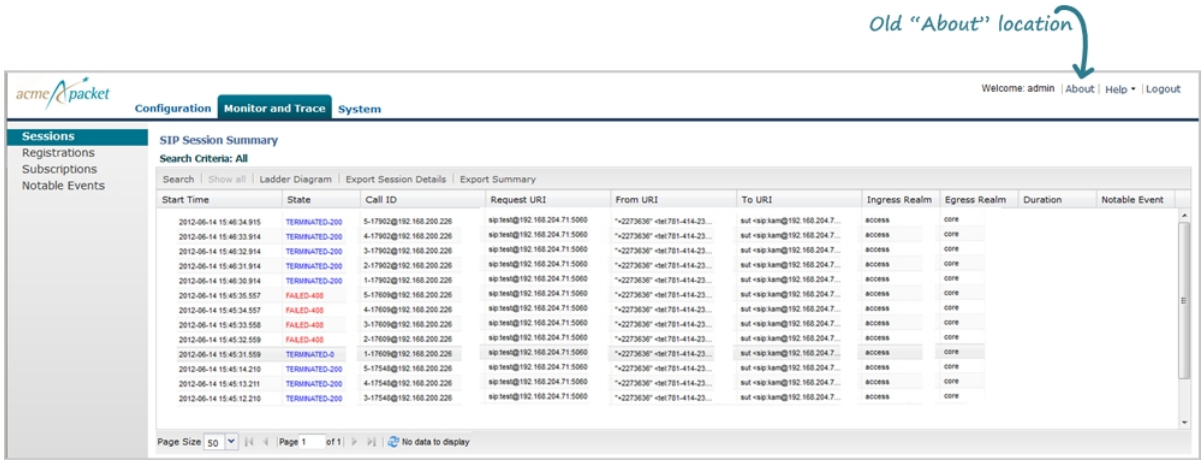
   Note: If needed, you can reinstall the backed up configuration at a later time from the System tab in the Web GUI.

3. Click **OK**.

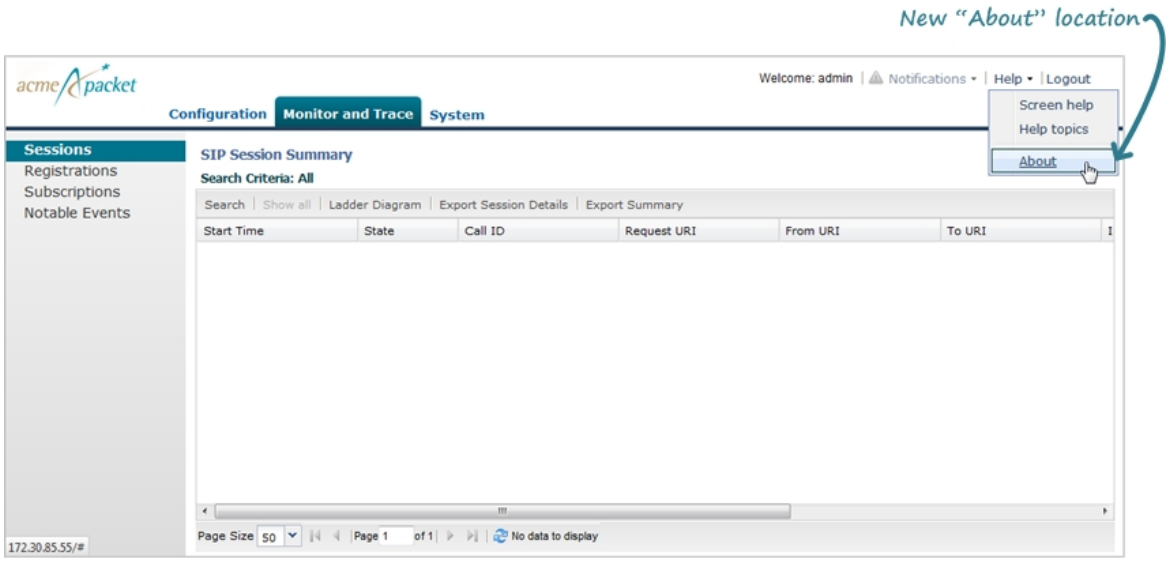
4. On the Configuration page toolbar, click **Save**.

About Link Under Help Menu

Previously, the About link was located at the upper right corner of the screen in the Web GUI.



The About link is now a selection under the Help Menu. The About link allows you to display the current version of software, as well as the licenses associated with the software.



ACLI Feature

The following ACLI feature is new in E-C[xz]6.4.0 M1.

New quit Command in Configuration Mode

Previously, when you finished a feature configuration in the ACLI, you would enter "exit" and hit <Return>. After entering "y" at the Save Changes [y/n]? prompt, the previous level prompt displayed.

In the following example, the "exit" command is used and the session-recording-server configuration is saved. The previous level prompt of session-router displays.

```
ACMEPACKET(session-recording-server)# exit
Save Changes [y/n]?: y
session-recording-server
        name                                    crs1
        description
        realm                                   1.1.1.1
```

```
        mode                                    selective
        destination                             2.2.2.2
        port                                    5060
        transport-method                        DynamicTCP
        ping-method
        ping-interval                           0
        last-modified-by                        admin@10.1.25.17
        last-modified-date                      2013-06-06 11:47:45
ACMEPACKET(session-router)#
```

In addition to the “exit” command, there is now a new quit command. When using the quit command, after saving a configuration, the configuration mode is exited and the root prompt for the Oracle Enterprise Session Border Controller displays.

In the following example, the “quit” command is used and the session-recording-server configuration is saved. The root prompt of ACMEPACKET displays.

```
ACMEPACKET(session-recording-server)# quit
Save Changes [y/n]?: y
session-recording-server
        name                                    crs2
        description
        realm                                   2.2.2.2
        mode                                    selective
        destination                             3.3.3.3
        port                                    5060
        transport-method                        DynamicTCP
        ping-method
        ping-interval                           0
        last-modified-by                        admin@10.1.25.17
        last-modified-date                      2013-06-06 11:49:24
ACMEPACKET#
```

Issues Resolved

The following table lists the problems resolved between Release E-C[xz]6.4.0 GA and Release E-C[xz]6.4.0 M1.

Description
Local Policy

Previously in the ACLI, you could not select the local-policy using the source-realm parameter value. The Oracle Enterprise Session Border Controller returned the error message "No matching entries". For example, if the source-realm value was “SD-Access” and you entered the following show command, the No matching entries error displayed:
`ACMEPACKET#: show running-config local-policy SD-Access`
`No matching entries found`
This is now corrected. In 6.4.0M1, You can now select the source-realm parameter value when selecting a local-policy.

Local Routing Table (LRT)
Previously, the Local Routing Table (LRT) range did not allow the following ranges: rangeEnd=9207218999 rangeStart=9207212000 These ranges in the LRT are now allowed.
Communication Monitor Probe
Previously, the internal save file format in the software was incorrect, so configuration values entered for the system-config->comm-monitor object did not work when loading/saving the configuration from other image versions. This is now corrected. Note: Before upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, see the Known Issues section for additional information about this fix.

Description
Timezone
Previously, the internal save file format in the software was incorrect, so the timezone-config object did not work when loading/saving the configuration from other image versions. This is now corrected. Note: Before upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, see the Known Issues section for additional information about this fix.
Accounting
Previously, the internal save file format in the software was incorrect, so configuration values entered for the account-config->interim-stats-id-type object did not work when loading/saving the configuration from other image versions. This has been corrected. Note: Before upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, see the Known Issues section for additional information about this fix.
H323
Previously, the internal save file format in the software was incorrect, so configuration values entered for the h323-stack->alternate-transport object did not work when loading/saving the configuration from other image versions. This has been corrected. Note: Before upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, see the Known Issues section for additional information about this fix.
Session Agent
Previously, the internal save file format in the software was incorrect, so configuration values entered for the session-agent->tcp-reconn-interval object did not work when loading/saving the configuration from other image versions. The range was off by a factor of 1000. This has been corrected.

Known Issues

The following table lists Release E-C[xz]6.4.0 M1 known issues and workaround steps.

Description	Workaround
Oracle Enterprise Session Border Controller Hardware	
Upon rebooting a DL320 G8 platform, a kernel crash with no restart may occur.	Do not configure VLAN on the media ports or Replace the Network Interface Card (NIC) that uses a Broadcom chip (tg3), with an Intel chip (igb), such as the HP Ethernet 1 Gb 2-port 361T Adapter (Vendor Part # 652497-B21), which is the recommended adapter.
Oracle Enterprise Session Border Controller hangs if a reboot is performed while the show support-info command is displaying results.	None
Web GUI/ACLI	
If you are changing the configuration on the Oracle Enterprise Session Border Controller server or VM via the ACLI, and then open a Web GUI session to that same server or VM, the Web GUI allows you to change the configuration even though you are configuring the server or VM via the ACLI. The Web GUI should	Only open one session at a time to the server or VM to configure it - either use the ACLI or use the Web GUI.

Description	Workaround
display an error message that prevents you from changing the configuration. This does not currently happen.	
Attributes with text fields are not accepting special characters like " " , ' '	Do not use special characters when adding text in the dialog boxes.
When in Basic Mode, and you restore an Expert Mode configuration using the System tab, an error occurs after switching to the Configuration tab.	None
SIP Monitoring and Trace (SMT) SIP traffic displayed in Session Details is missing the 'Via' header.	None
LDAP	
LDAP ACLs are not dynamically updated for multiple LDAP servers.	None
When configuring the "ldap-cfg-attributes" element at the path, session-router->ldap-config->ldap-transactions->ldap-cfg-attributes, you MUST specify a value for the realm attribute in order for calls to be received correctly.	When configuring the ldap-cfg-attributes element, specify a realm to which this configuration applies. For example: ldap-cfg-attributes name msRTCSIP-Line next-hop sag:SA1 realm net1651 extraction-regex ^\+?1?(\d{2})(\d{3})(\d{4})$ value-format tel:+1$1$2$3
SIP KPML Interworking	
Once Key Press Markup Language (KPML)-2833 interworking is negotiated, the Oracle Enterprise Session Border Controller is not sending out a SUBSCRIBE message.	None
Communication Monitor Probe	
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for system-config->comm-monitor->local-intf in 6.4.0 GA disappear in 6.4.0 M1.	Make a note of your configuration settings for system-config->comm-monitor->local-intf and reconfigure these settings after the upgrade to E-C[xz]6.4.0 M1 is complete.
Timezone	
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for timezone-config in 6.4.0 GA disappear in 6.4.0 M1.	Make a note of your configuration settings for timezone-config and reconfigure these settings after the upgrade to E-C[xz]6.4.0 M1 is complete.
Accounting	
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for accounting-config->interim-stats-id-type in 6.4.0 GA disappear in 6.4.0 M1.	Make a note of your configuration settings for accounting-config->interim-stats-id-type and reconfigure these settings after the upgrade to E-C[xz]6.4.0 M1 is complete.
H323	

Description	Workaround
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for h323-stack->alternate-transport in 6.4.0 GA disappear in 6.4.0 M1.	Make a note of your configuration settings for h323-stack->alternate-transport and reconfigure these settings after the upgrade to E-C[xz]6.4.0 M1 is complete.
Session Agent	
After upgrading E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, or downgrading from E-C[xz]6.4.0 M1 to a previous version, the saved configuration settings for session-agent->tcp-reconn-interval disappear.	Make a note of your configuration settings for session-agent->tcp-reconn-interval and reconfigure these settings after an upgrade to E-C[xz]6.4.0 M1, or after a downgrade from E-C[xz]6.4.0 M1 to a previous version.
Historical Data Recording (HDR)	
In Release E-C[xz]6.4.0 GA and above, the “start-time” and “end-time” objects at the path: system->system-config->collect->group-settings, does not derive the values from the global “start time/end time”. Instead, the “start-time” always has a value of “now” and “end-time” always has a value of never for individual groups.	You must manually configure this start-time/end-time for individual groups if values other than the defaults are required. Note: For more information on configuring the collector, see the Net-Net C-Series Historical Data Recording (HDR) Resource Guide, Version S-CX6.4.0.

Limitations

The following table lists limitations in Release E-C[xz]6.4.0 M1.

Limitation
Web Server
High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
For configurations that contain 2000 or more realms, after logging into the Web GUI and clicking on realm-config in Expert Mode, the configuration may take up to 20 seconds to load.
Hyper-V
The following are specific limitations when using Hyper-V: - Limited session capacity when using Hyper-V Hypervisor (50 media sessions). - Network booting is not supported due to Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adapters". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.

2

E-C[xz]6.4.0 M2

Platforms Supported

Release E-C[xz]6.4.0 M2 runs on the following platforms:

- Oracle Hardware: Net-Net 3820, Net-Net 4500
- Server Edition (SE): HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition (VME): VMWare and Hyper-V

Software Images

This section describes software images for this release.

For Acme Packet Hardware

If you are using Oracle hardware, use the following software image: nnECX640M2.tar. The X in the file name corresponds to Oracle hardware.

The latest software is packaged in .tar format. Older releases were packaged as .xz format. When upgrading from releases previous to 6.3.9, please assure bootloader build date is 1/19/2012 or newer. You can download the most recent bootloader from the Oracle support site: support.acmepacket.com.

All Other Hardware or Software-only

If you are using hardware other than Oracle's or running this software as a VM, use a file defined in this section for your needs. The Z in the file name corresponds to non-Oracle hardware or VM.

- Single system image file: nnECZ640M2.bz
- Boot Media Creator: nnECZ640M2-img-usb.exe
- Virtual Machine VMWare: nnECZ640M2-img-bin.ova
- Virtual Machine Hyper-V: nnECZ640M2-img-bin.vhd

For software-only options, the following file is pre-loaded on the USB stick for [Z] builds: SWR-0028-00.tar.

Browser Support

You can use any of the following Web browsers to access Oracle’s web GUI:

- Internet Explorer versions 9.0 and higher

- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle Enterprise Session Border Controller software, you should clear your browser cache before using the Oracle Enterprise Session Border Controller web GUI.

Content Map

The following table identifies the new features in Release E-C[xz]6.4.0 M2.

Content Type	Description
Adaptation	Web GUI Enhancements
Adaptation	1663 - Remote Site Survivability
Adaptation	4216 - P-Certificate-Subject-Common-Name to REGISTER Messages
Adaptation	4173 - Web GUI Session-Agent Column Enhancement
Adaptation	SIP Monitor and Trace Enhancements
Adaptation	ELIN Gateway Support
Adaptation	Avaya SM Dual Registration Support
Library updates	Update to latest version of OpenSSL library Updates SPL engine to version C2.0.2
Licensing	Licensing information was removed from the USB dongle.

New Features

This section lists the new features available in E-C[xz]6.4.0 M2:

Web GUI Enhancements

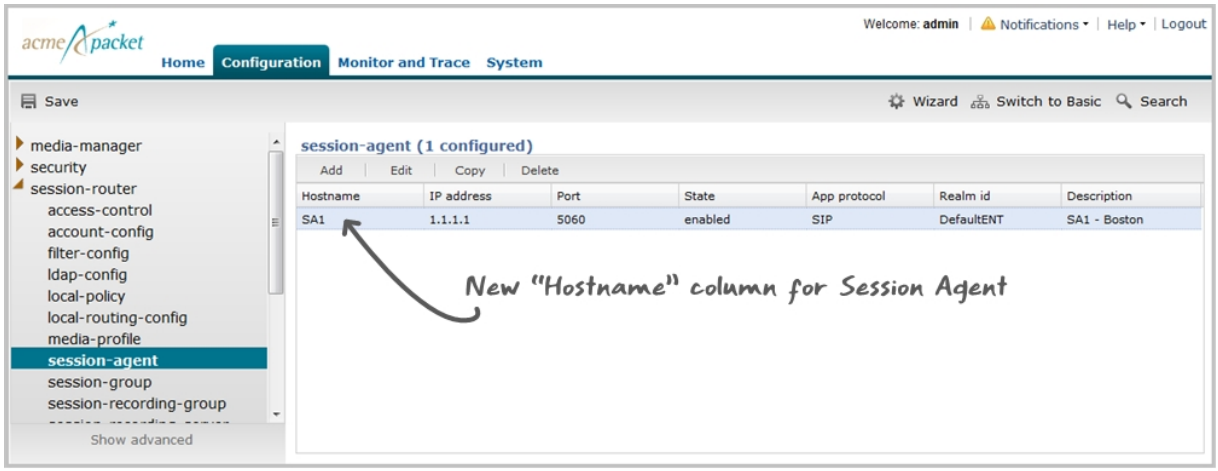
This section provides information about the Web GUI enhancements in Release E-C[xz]6.4.0 M2.

Web GUI Session-Agent Column in Expert Mode

Previously, the session-agent page in Expert mode in the Web GUI did not display the Session Agent name after adding a Session Agent.

Release E-C[xz]6.4.0 M2 now displays a Hostname column under the session-router->session-agent page when you add a session-agent.

The following shows the Hostname column on the Session Agent page.

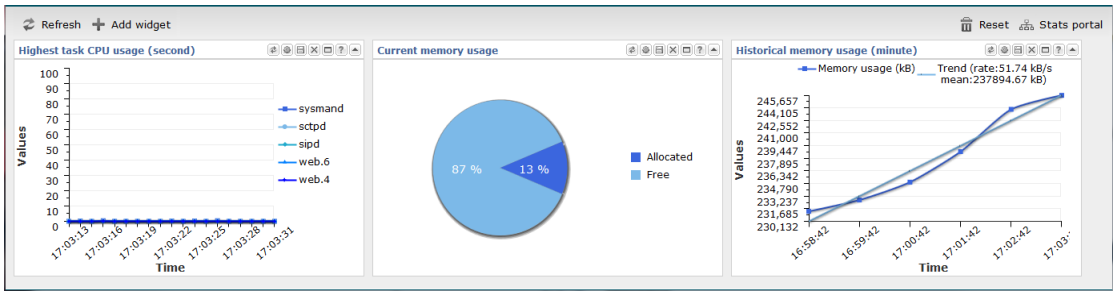


New Home Page in Web GUI

Release E-C[xz]6.4.0 M2 offers the ability to display Session Initiation Protocol (SIP) statistics on a new Home tab in the Oracle Enterprise Session Border Controller (E-SBC) Web GUI.

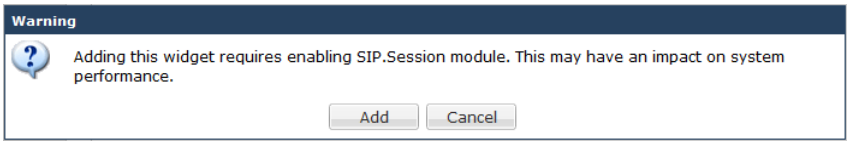
After logging into the E-SBC Web GUI, the Home page displays showing the following tables by default:

- Line graph of Highest CPU Usage
- Pie graph of Current Memory Usage
- Line graph of Historical Memory Usage



This page is called the “Dashboard” on the Web GUI. Each of the tables is called a widget, which contains specific statistics about the E-SBC. You can customize the Dashboard by adding, deleting, and moving the widgets. You can also refresh the statistics on the Dashboard, or return (reset) the Dashboard back to its default table display as shown above.

The operation of some widgets can degrade system performance. Examples of these widgets include those that require the SIP.Session module enabled. These widgets are not included on the default Dashboard. When you add one of these widgets to your home page, the system displays the following Warning dialog allowing you to add the widget or cancel the operation. Add these widgets only within a window in which the performance impact does not degrade service.



The system displays this dialog once per module that you enable. The performance impact of multiple widgets using that module is not additive. Be sure to monitor CPU usage when you enable modules that degrade system performance.

Note: The E-SBC collects only SIP data for the dashboard widgets, including the default CPU and Memory widgets. For this reason, you must set up a valid SIP configuration before the E-SBC can display any data on a dashboard widget.

The following table describes the buttons you can use on the Dashboard page to customize your display.

Buttons	Description
Refresh	Updates all of the statistics in the widgets that currently display on the Dashboard.
Add widget	Displays a list of all widgets from which you can select to add to the Dashboard.
Reset	Resets the Dashboard to display the default widgets of: SIP Media Flow line graph Current Memory Usage table list Current Memory Usage pie graph All other previous widgets are removed from the Dashboard.
Stats portal	Displays the widget groups and subgroups. This portal allows you to display the statistics for a widget in either table or graph presentation. After selecting a widget for display, you can also perform the following for that widget: Refresh widget statistics Change widget settings Export widget statistics to a .csv file Add a widget to the Dashboard Display help for that widget For more information about the functions you can perform when a widget is displayed in the Stats Portal, see *Stats Portal Widget Tools* .

Types of Widgets

The following tables describe the types of widgets that you can add to the Dashboard to display Command, Session Initialization Protocol (SIP), and System, statistics.

Command Widget	Description
Show Configuration	Displays either the running configuration or the editing configuration for the selected configuration.

SIP Widget	Description
Message - Requests per second	Displays the number of requests per second.
Message - Response	Displays the number of responses per second.

SIP Widget	Description
Session - Answer Seizure Ratio (ASR)	Displays the percentage of answered calls with respect to the number of calls attempted during a period of time.
Session- Duration	Displays the total number of sessions and their durations.
Session - Established	Displays the number of sessions established during a period of time.

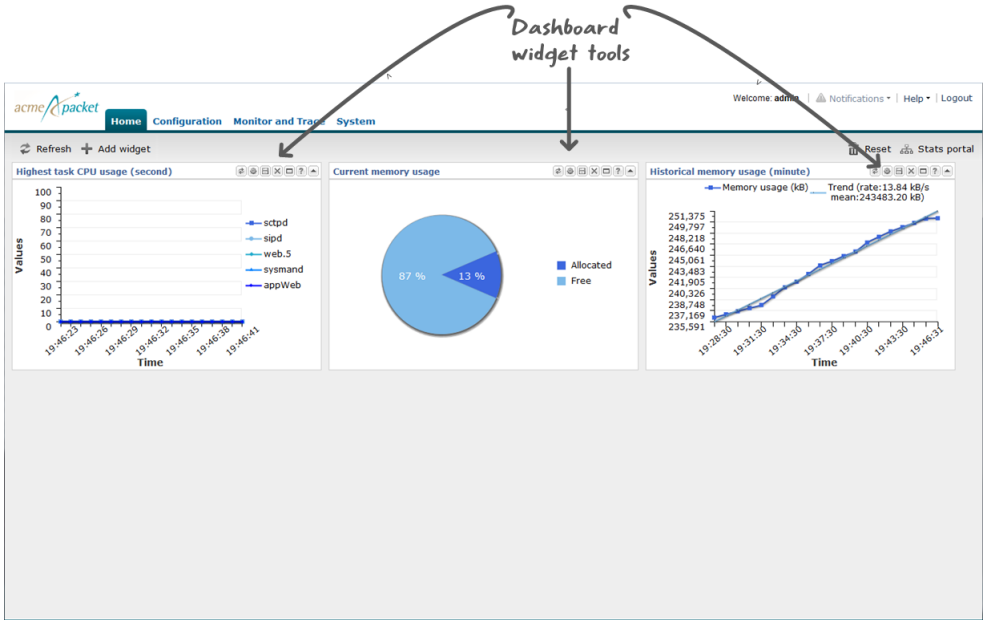
System Widget	Description
Alarms	Displays configured alarms and allows the user to clear the alarms.
Configuration Inventory	Displays a list of changes made to configuration elements. The display shows the Running Count and counts for the following types of Changes Not Activated. • Total • Added • Modified • Deleted A selectable filter can change the display from Total count to the difference between the Running Count and the Changes Not Activated Count.
Configuration Version	Displays the version number that is configured and the version number that is running.
CPU Usage	Displays 5 to 10 tasks with the highest percent of CPU usage during a period of time.
Current Disk	Displays the disk usage for the code directory on the Oracle Enterprise Session Border Controller. The system uploads data from the Web GUI to the code directory.
Current Memory	Displays the current percentage of free memory.
Historical Memory	Displays the number of kilobytes of free and allocated memory over a period of time.
System Health	Displays the synchronization health of the following components. • Collect • Config • Media • Media Gateway Control • RADIUS Call Detail Record (CDR) • REC • Rotated Call Detail Record (CDR) • Service Health • SIP
User Management	Displays the user's remote IP address, duration, type, state, and user name.

Dashboard

This page is called the "Dashboard" in the Web GUI. Each of the tables is called a widget that contains specific statistics about the Net-Net Enterprise Session Director. You can customize the Dashboard by adding, deleting, and moving specific widgets. You can also refresh the statistics on the Dashboard, or return (reset) the Dashboard back to its default display.

Note:

You must have a valid SIP configuration on your Net-Net ESD to display the statistics on the Dashboard. The Net-Net Enterprise Session Director collects only SIP data (sipd) for these widgets, including the CPU and memory widgets.



The following table describes each icon on the Dashboard widget.

Description
Refresh Update the statistics displayed on the widget.
Settings Configure display settings for the widget, such as: • Auto-Refresh Interval • Table Name

Description
Settings Note: The Table Name setting applies only to specific widgets.
Export Export the data from the widget to a .csv file. The data in the .csv file displays in table format.
Remove Remove the widget from the Dashboard.
Enlarge Enlarge the widget on the screen and place it on top.
Help Displays a short description of the selected widget.
Minimize Minimize the widget on the Dashboard.
Maximize Maximize the widget on the Dashboard.

Adding and Moving Widgets

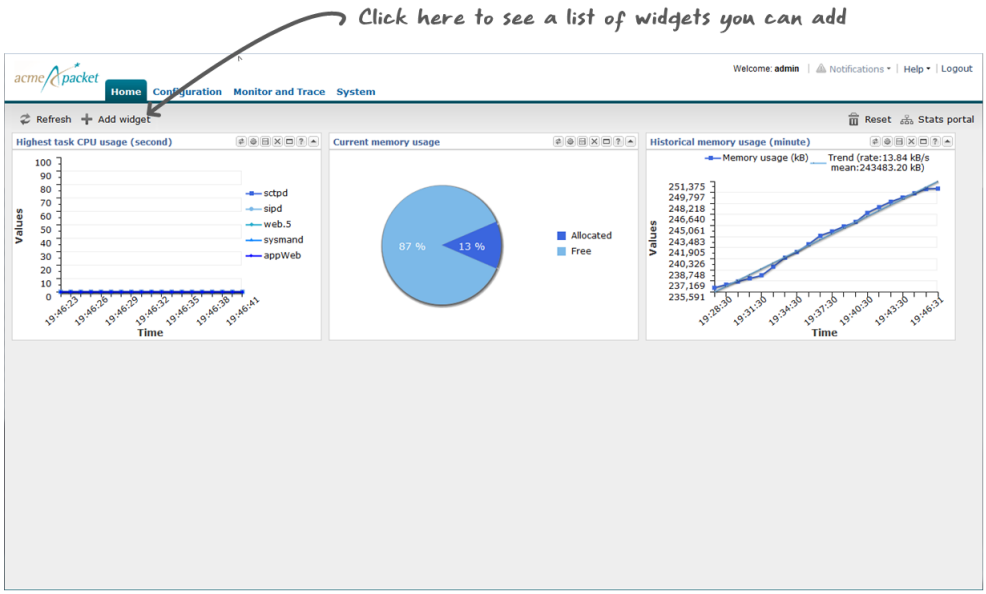
You can add an unlimited number of widgets to the Dashboard. As you add widgets, the new widgets are added to the first vertical column. When the first column reaches its maximum potential, the widgets are added to the vertical second column. When the second column reaches its maximum potential, the widgets are added to the third column, and so on.

As the widget fills a column, a scroll bar appears on the right of the Dashboard to allow scrolling up and down to view the widgets in that column. When additional columns are required for widgets, a scroll bar appears at the bottom of the Dashboard that allows you to scroll right and left to view the columns of widgets.

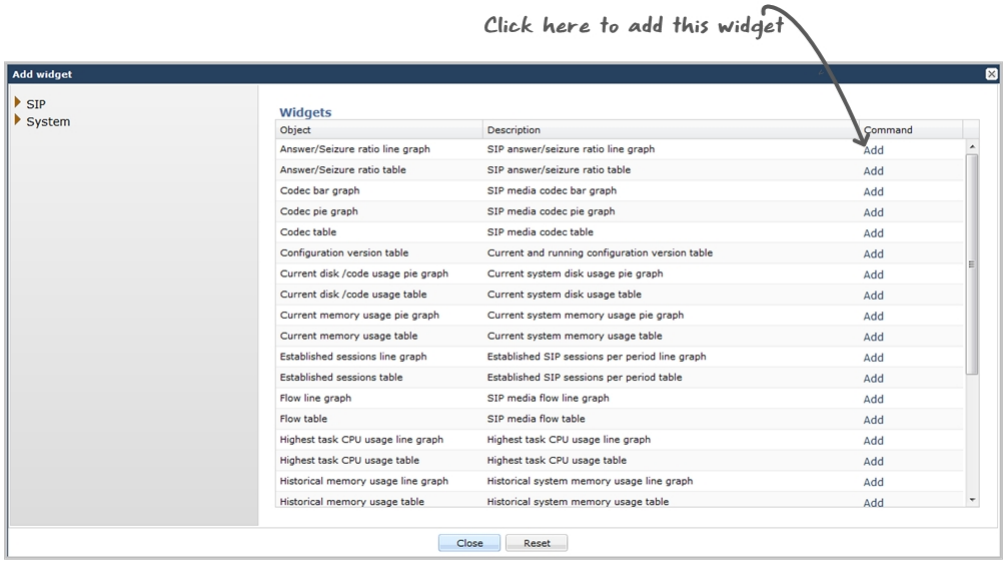
You can move a widget from one location in the dashboard to another (up/down or right/left) by dragging and dropping it within the columns.

To add a widget to the Dashboard:

1. From the Dashboard, click <Add widget>.



The following pop-up displays.



This page shows the groups and subgroups presented as a menu tree. If you select a group or subgroup, the widgets display in the right column.

2. In the menu tree, select a SIP or System group or select a subgroup.
3. Select a widget from the subgroup, or click on a widget that displays in the right column.
4. Click Add to add that widget to the Dashboard. The list of widgets remains displayed so you can add other widgets if required.
5. Click <Close> to close the list of widgets. The Dashboard displays the widgets you just added.

Note: You can click <Reset> if required, to set your Dashboard back to its default widgets.

Next Steps

Configure widget display settings.

Configure Data Sampling Settings for a Dashboard Widget

To see SIP and System statistics displayed on a Dashboard widget, the system requires a setting for how often to refresh the display. You can use the default interval or select one from the Auto-refresh interval drop-down list on the widget. Some widgets also display the Table Name drop-down list, where you can set the data sampling frequency. For example, you might configure the widget to refresh the display every 40 seconds and to display the data samples in one minute increments.

Before you begin, confirm that the widget that you want to configure is on the Dashboard. See *Add a Widget*.

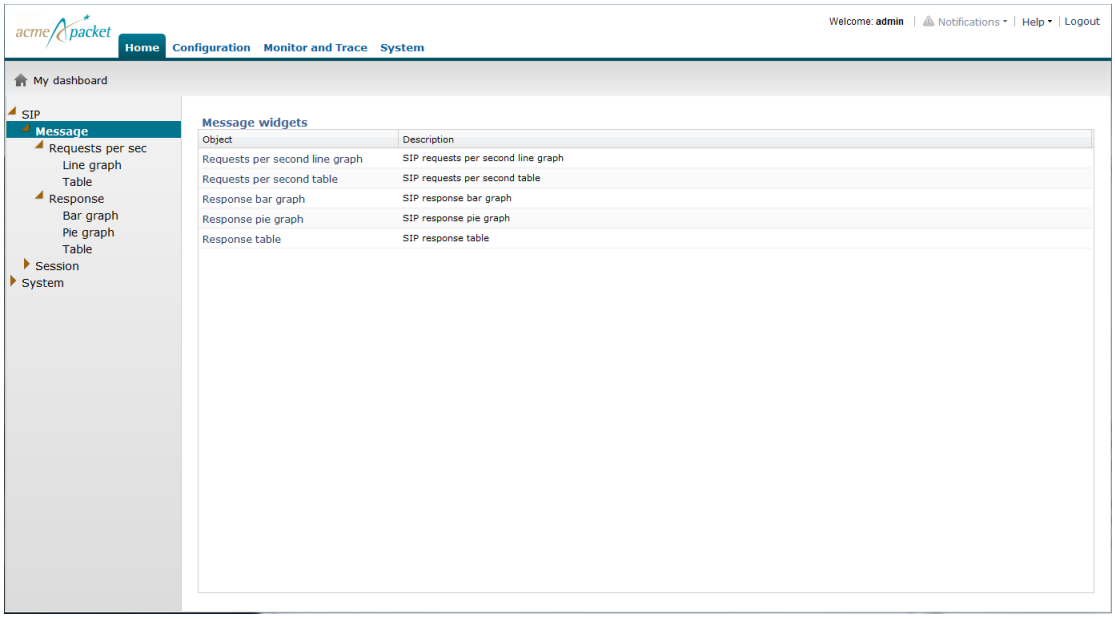
1. On the Dashboard, click the **Home** tab.
2. On the widget, click the **Settings** icon.
3. Select a widget display refresh frequency from the **Auto-Refresh Interval (seconds)** drop down list.
4. If the widget displays the **Table Name** drop-down list, select a data sampling increment for the widget display.
5. Click **OK**.

Accessing the Stats Portal

You can access the Stats Portal to display the SIP and System groups and subgroups presented as a menu tree. This portal allows you to display the statistics for a widget in either table or graph full-screen presentation.

To access the Stats Portal:

1. In the upper right corner of the Dashboard, click Stats Portal. The following displays.

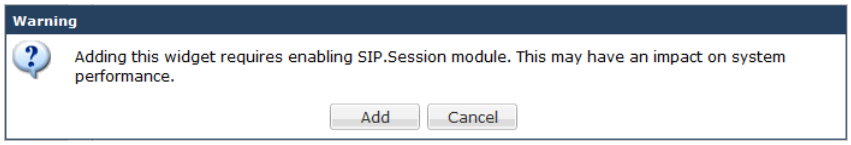


This page shows the groups and subgroups presented as a menu tree. If you select a group or subgroup, the widgets display in the right column.

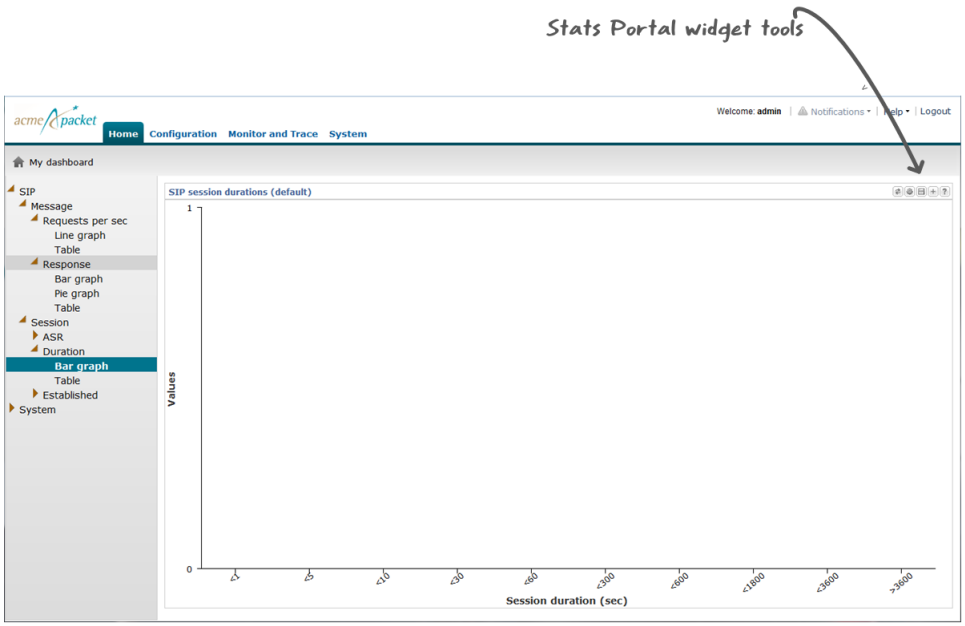
2. In the menu tree, select a SIP or System group or select a subgroup.
3. Select a widget from the subgroup, or click on a widget that displays in the right column. The widget you select displays as a full-screen presentation.

   The system allows access to widgets depending on their applicable module's status on the home page - enabled or disabled. If the widget is not yet added to the home page, the system provides a dialog box from which can enable the applicable module or cancel the operation.

   Recall that some widgets' module can degrade system performance. If you attempt to add one of these widgets, the dialog warns you of this system performance impact.



The widgets that display in the Stats Portal provide specific tasks you can perform with the statistics in each widget.



The following table provides a description of each tool in the Stats Portal widget.

Tool	Description
	Refresh - Allows you to update all of the statistics that currently display in this widget.
	Settings - Allows you to configure specific settings that affect the display of the widget. Settings include: Table Name Auto-Refresh Interval Note: The Table Name setting is applicable to specific widgets only.
	Export - Allows you to export the data from the current widget to a .csv file. The data in the .csv file displays in table format.
	Add - Allows you to add the current widget to the Dashboard. After clicking this tool, the message Successfully added to Dashboard displays.

Tool	Description
	Help - Displays a short description of the current widget.

Home Tab Screen Help

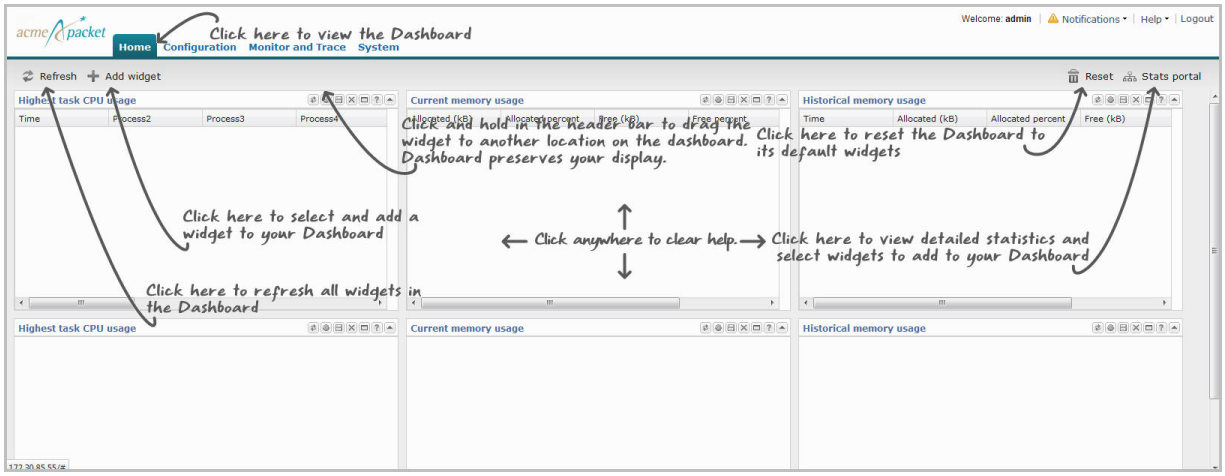
Screen Help provides an overlay on the current screen with pointers that indicate specific tasks you can perform. When you select Help->Screen help in the upper right corner of the page, an overlay displays with screen pointers to specific areas of the blurred-out screen. Clicking anywhere on the screen closes this help method.

You can display screen help on the Home page for the Dashboard and for the Stats Portal. Use the following procedure to display Screen Help.

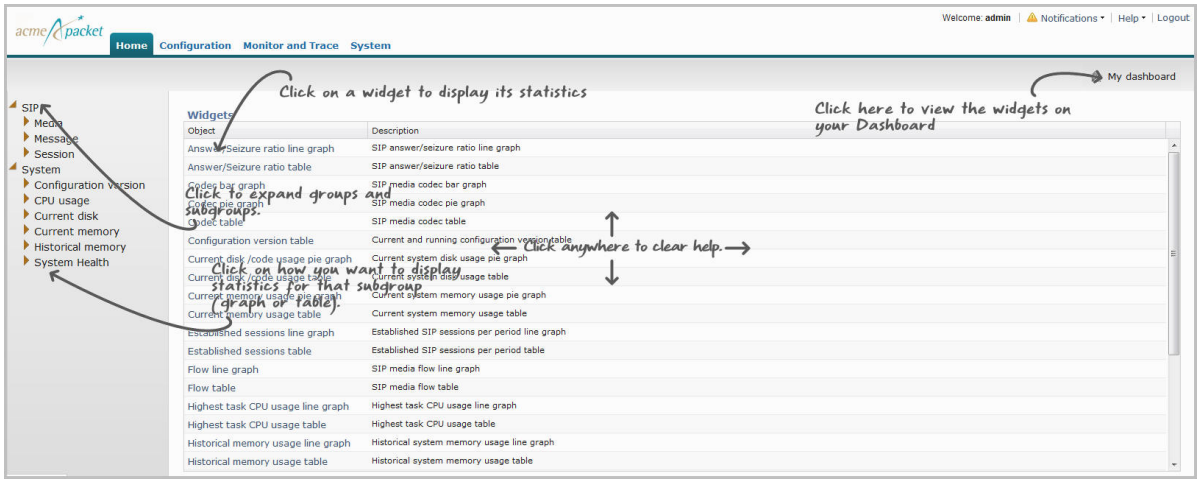
To display Screen Help:

1. After logging into the Web GUI, click the Home tab.
2. Select Help->Screen help in the upper right corner of the screen. An overlay displays on the screen with help pointers to tasks you can perform. The following illustrations show the screen help for the Dashboard and for the Stats Portal.

   Home Tab (Dashboard)



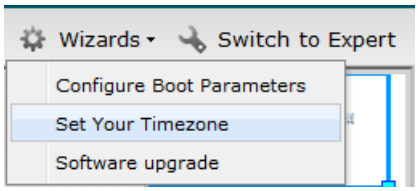
   Home Tab (Stats Portal)



Configuration Wizards

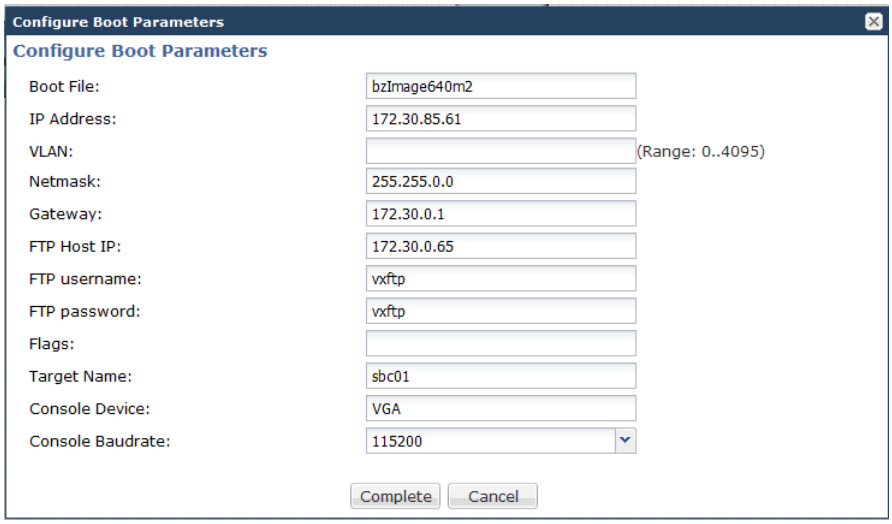
Configuration wizards are GUI-based configuration dialogs that step the user through key configuration procedures, simplifying the procedure for the user.

To run configuration wizards, click the Wizards pull down from the upper right-hand region of your home page. The system displays the following dialog



The system provides the following wizards within this release:

- Setting Your Timezone - Displays a simple dialog from which you pick your desired timezone from a drop-down list.
- Software upgrade - Displays the same dialog available from the system tab, allowing you to upgrade your software image. All fields are documented in this document's Upgrade Software with the GUI section.
- Configure Boot Parameters - Displays the dialog shown below, from which you can change your system's boot parameters. All fields are documented in the *Net-Net Enterprise Session Director Configuration Guide*.



To perform these configurations, fill in the fields as desired and click the "Complete" button.

Upgrade Software with the GUI

Previously, software upgrade was a manual process consisting of file transfer tools and ACLI procedures. Release E-C[xz]6.4.0 M2 now allows you to upgrade software directly from the GUI.

You can upgrade (or downgrade) the software on your system from the GUI's System tab. The function is found via the Upgrade Software link. It performs the following tasks for you:

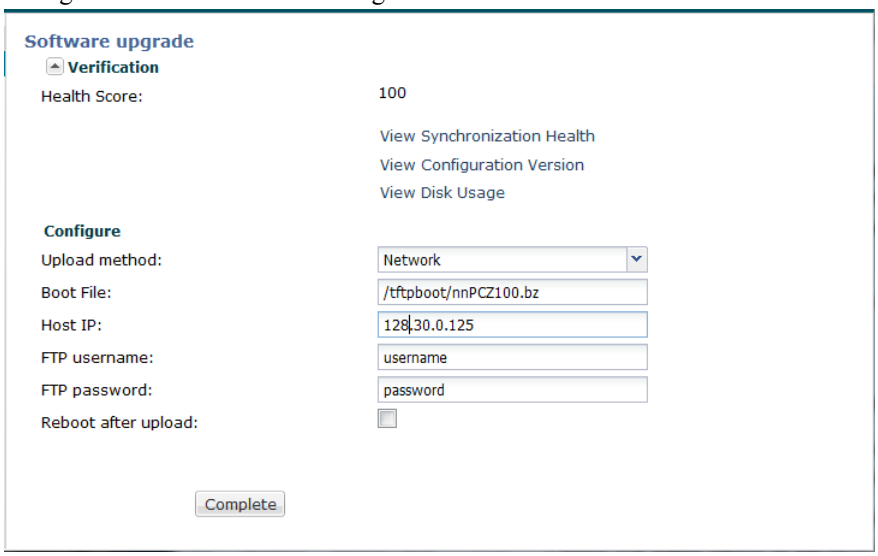
For standalone system upgrade:

- System Health Score Display
- System Disk Space Check
- Display Current CFG Version
- Display Current Running Version
- File Transfer from Local System
- Change Boot Parameters
- System Reboot

For High Availability configuration upgrade, the system displays the synchronization health.

This procedure assumes SFTP access between your device the source of your new software. Follow the steps below to perform a software upgrade:

1. Click the System tab.
   The system opens the System dialog.
2. Click the Upgrade Software link.
   The system displays the upgrade software dialog.
3. Open the Verification menu.
   The system displays the current system health and links from which you can assess synchronization health, current configuration version and disk usage.



4. Verify that system health, synchronization health, current configuration version and disk usage are appropriate and adequate for you to proceed with your upgrade.
5. Select the Upload method from the drop-down box. Options include.

   - Local - Allows you to select a file from your system for transfer.
   - Flash - Allows you to select a file already on the device.
   - Network - Allows you to specify parameters for network boot via file transfer. These parameters initially display the current boot parameters.

   The system updates the Upgrade Software dialog with the fields you need for your selection.
6. Complete the fields, specific to your current upgrade.

   - Software file to upload - (Local) Use the Browse button to locate the file on your local system.
   - Software file - (Flash) the location and name of the file on the device.
   - Boot file - (Network) The complete name of the boot file.
   - Host IP - (Network) The IP address of the FTP server.
   - FTP username - (Network) The username to log into the FTP server.
   - FTP password - (Network) The password to log into the FTP server.
7. Click the Reboot after upload checkbox, if desired.
8. Click the Complete button.
   If you did not check the Reboot after upload checkbox, the system displays an information dialog indicating that the it needs to reboot for changes to take effect. If you did check the Reboot after upload checkbox, the system displays an information dialog indicating that it is about to reboot.
9. Click OK.
   The system performs the file transfer or boot parameter change and, if selected, reboots.

Managing Certificates from the Web GUI

Previously, certificate management was a manual process consisting of file transfer tools and ACLI procedures. Release E-C[xz]6.4.0 M2 now allows you to manage certificates directly from the GUI. These procedures include:

- Creating Certificate Records

- Generating Certificate Requests
- Importing Certificates

Each of the procedures are described in the subsection below.

Access to certificate management dialogs is dependent on configuration mode.

- Basic mode - Expand the security menu. Then click the certificate-record link.
- Expert mode - Click the Security icon to display the security menu. Then click the certificate record link.

Both of these procedures display the certificate record dialog.

Certificate Record Configuration

A certificate record configuration represents either the end-entity or the Certificate Authority (CA) certificate on the Oracle Enterprise Session Border Controller. If it is used to present an end-entity certificate, a private key should be associated with this certificate record configuration using a certificate request. No private key should be associated with the certificate record configuration if it was issued to hold a CA certificate.

A certificate can be imported to a certificate record configuration using the GUI as described below.

Note: There is no need to create a certificate record when importing a CA certificate or certificate in pkcs12 format.

Follow the steps below to create a certificate record.

1. Access certificate configuration controls via the Security link.
2. Click the link indicating **Certificate** configuration. The system displays the list of certificate records already configured on this system.
3. Click the **Add** link. The system displays the Add Certificates dialog. Note that this dialog is truncated for presentation purposes here.
4. name—Enter the name of the certificate record. This parameter is required; you cannot leave it empty.

   In the case of establishing a certificate for the Oracle Enterprise Session Border Controller, this name must be the same as the name you use to generate a certificate request.

   If configuring for an end stations CA certificate (mutual authentication), this name must be the same name used during the import procedure. When performing an import procedure that creates the record automatically, this name will be derived from the certificate itself.
5. country—Enter the name of the country. The default is US.
6. state—Enter the name of the state. The default is MA.
7. locality—Enter the name of the locality for the state. The default is Burlington.
8. organization—Enter the name of the organization holding the certificate. The default is engineering.
9. unit—Enter the name of the unit within the organization holding the certificate.
10. common-name—Enter the common name for the certificate record.
11. key-size—Enter the size of the key for the certificate. Use the default of 1024, or change it to one of the other supported values: 512, 2048, or 4096.
12. alternate-name—Enter the alternate name of the certificate holder.
13. key-usage-list—Enter the usage extensions you want to use with this certificate record. This parameter can be configured with multiple values, and it defaults to the combination of digitalSignature and keyEncipherment. For a list of possible values and their descriptions, see the section “Key Usage Control” in the *Oracle Communications Session Border Controller Configuration Guide*.
14. extended-key-usage-list—Enter the extended key usage extensions you want to use with this certificate record. The default is serverAuth. For a list of possible values and their descriptions, see the section “Key Usage Control” in the *Oracle Communications Session Border Controller Configuration Guide*.

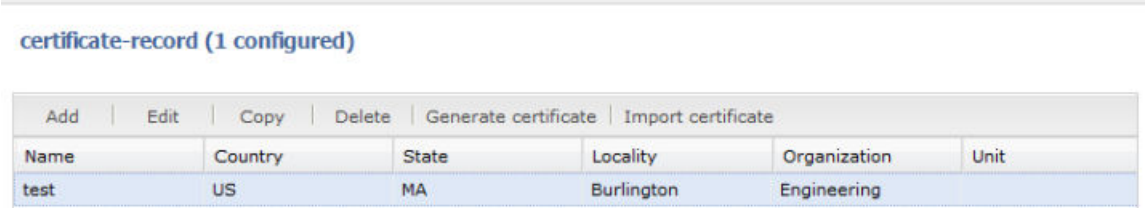
Create TLS profiles, using your certificate records to further define the encryption behavior and provide an entity that you can apply to a SIP interface.

Generating a Certificate Request from the GUI

To operate with a certificate authorized by a CA, you provide a certificate request to that CA. To do this, you create a certificate record and generate the request from this record.

You can generate a certificate request using the ACLI or the GUI. This procedure provides the steps you use on the GUI.

1. Highlight the certificate record you created for the purposes of containing your device's certificate.



2. Click the Generate certificate link.
   The system creates the request and presents it to you in a dialog.

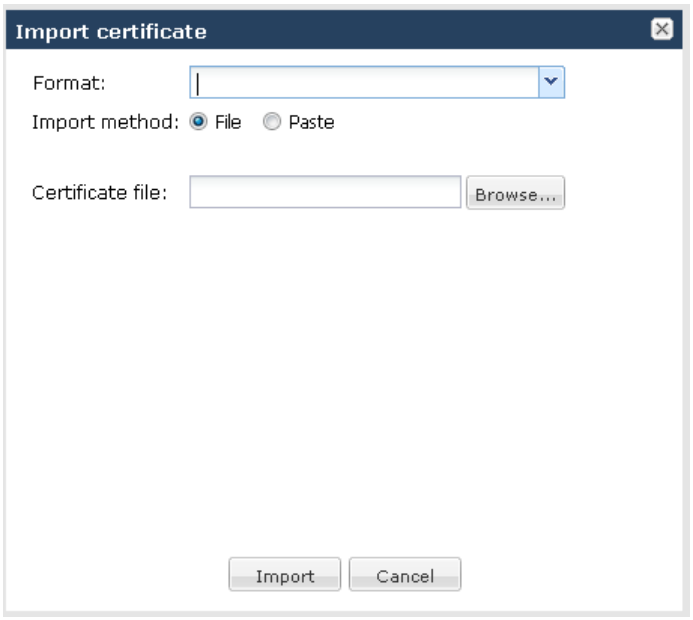
3. Copy the information from the dialog and send to your CA as a text file.

When the CA replies with the certificate for your device, import this certificate to the device against the same certificate record. This allows end stations to establish TLS paths within either server or mutual authentication scenarios.

Importing Certificates

Use this procedure to import both your device certificate and end station CA certificates for mutual authentication scenarios. Recall that you must import your Oracle Enterprise Session Border Controller certificate against the certificate record you created for your Oracle Enterprise Session Border Controller. End station CA certificates may or may not need to be imported against a pre-configured certificate record.

1. If applicable, highlight the certificate record for which this certificate applies.
2. Click the Import certificate link.
   The system responds with a dialog from which you can either import the certificate file directly or paste the contents of the certificate.
3. Select the Format of the certificate from the drop down list. Options include:
   - pkcs7
   - x509
   - Try-all, which attempts to import via all possible formats until it is able to import the certificate.
4. Either browse to and select the certificate file, or click the paste button to change the dialog to its "paste format". This "paste format" provides a text field into which you paste your certificate information



5. Click the Import button.
   The system completes the procedure by importing the certificate.

Apply the operational certificate record to the intended SIP interface.

Remote Site Survivability

Release E-C[xz]6.4.0 M2 includes a new feature called Remote Site Survivability. This feature is the Oracle Enterprise Session Border Controller's ability of a Remote Office/Branch Office (ROBO) to detect the loss of communication over SIP-based telephony, to the Enterprise's core call processing Data Center. When loss of communication is detected over the SIP service, the ROBO Oracle Enterprise Session Border Controller dynamically switches into Survivable Mode, locally handling call processing and providing limited additional server functionality.

Note: Remote Site Survivability supports SIP only. It does not support the H.323.

The following are features of Remote Site Survivability:

- Works with or without High Availability (HA) operation.
- Configurable in real-time - no reboot required to enable this feature.
- Allows configuration of the feature via the Oracle Enterprise Session Border Controller Web GUI
- Maintains Historical Recording (HDR) statistics about being in survivability mode, such as:

  Whether or not the Oracle Enterprise Session Border Controller is in survivable mode using the ACLI command, show health.

  Length of time the Oracle Enterprise Session Border Controller was in survivable mode (records number of times and amount of time in survivability mode)

  Number of SIP messages handled in survivable mode

  Number of SIP users registered locally in survivable mode (both existing based on cache, and separately - new registrations).

How it Works

When configured for Survivability, the Oracle Enterprise Session Border Controller operates in either normal or survival mode. In normal mode, the IP wide area network (WAN) connection between the remote Oracle Enterprise Session Border Controller and the data center headquarters site is operational, and endpoints at the remote site register through the SBCs to an IP-PBX or Application Server (AS) at headquarters. Similarly, the Net-Net ESD forwards

calls between endpoints to the IP-PBX or AS at headquarters. When an endpoint registers, the Oracle Enterprise Session Border Controller inserts a registration entry for the endpoint in its local registration cache.

When the IP connection to headquarters goes down, the Oracle Enterprise Session Border Controller operates in survival mode. In this mode, the system is able to detect any loss of connection (and subsequent re-connection) to the core data center based on a health score (For more information about health score, see *Survivability Health Score*). When it detects a loss of connection, it enters survival mode and locally processes registrations and session traffic without routing them to the registrar. The Oracle Enterprise Session Border Controller also handles call routing in this mode. When a subsequent re-connection is detected, the system exits survival mode and proxies all registrations and session traffic once again to the data center (normal mode).

In "Survival Mode", the ROBO Oracle Enterprise Session Border Controller provides the following capabilities:

- Maintains SIP registrations for local SIP phones (based on existing registration cache).
- Provides local extension-to-extension calling and incoming public switched telephone network (PSTN), if available, to local extension dialing.
- Provides extension-to-PSTN calling through a media gateway (assuming a gateway is available) or alternatively, via a configured SIP trunk/route.
- Allows all new registration requests (without authentication) to be successful.
- Allows extensions to be dialed based on its multiple user identities (either identified by using P-Asserted-Identity or BroadSoft's proprietary mechanism). For more information about Survivability using a BroadSoft server, see *Remote Site Survivability with a BroadSoft Server*.

Survivability Health Score

When Survivability Mode is enabled on the Oracle Enterprise Session Border Controller, the system is able to detect any loss of connection (and subsequent re-connection) to the Enterprise's core data center based on a health score.

For the purpose of health monitoring, a sip-interface and one or more attached session agents can be logically grouped together by configuring a"service-tag" parameter to indicate the name of the session agent group. The service health score of the group is based upon the health status of the session agents within the group and can be configured using the session-agent-health parameter. The session-agent-health score can be a value between 0 and 100.

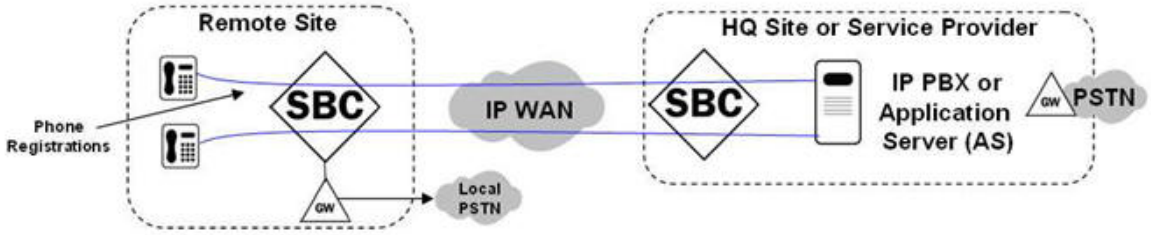
The determination of when to enter survival mode is determined by the session agent health score. The session-agent-health value is the amount that is deducted from the service health score when the session agent goes out of service. The sum of the service health values of all session agents assigned to a specific service tag must equal 100 to stay in normal mode. In cases where there is one session agent, the service health value is 100. For cases where there are two session agents, each session agent could have a service health of 50.

When the service health score goes down to zero the Oracle Enterprise Session Border Controller enters survival mode. While in survival mode, the Oracle Enterprise Session Border Controller continuously attempts to re-establish communications with the session agents. If communication is re-established, the Oracle Enterprise Session Border Controller adds the service agent health value of the session agent to the current service health score, and survival mode is exited if the service health score is above zero.

Note: For more information about configuring Survivability Mode and the Survivability health score, see *Configuring Remote Site Survivability using the ACLI* or *Configuring Remote Site Survivability using the Web GUI*.

Normal Behavior Call Process

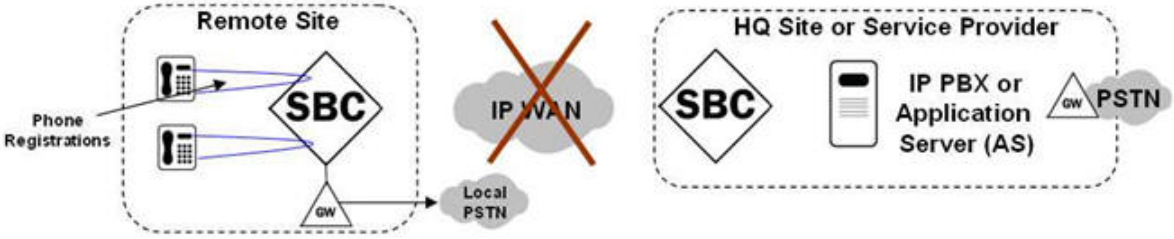
The following illustration shows the normal call process behavior of the ROBO
Oracle Enterprise Session Border Controller connectivity to the Service Provider site (or headquarters site).



1. Phones register through the Oracle Enterprise Session Border Controller to the IP PBX or Application Server (AS) at the Headquarters or Service Provider site.
2. Phone-to-phone calls are proxied through the Oracle Enterprise Session Border Controllers to the IP PBX or AS at the Headquarters or Service Provider site.
3. Phone-to-Public Switched Telephone Network (PSTN) calls are routed to the Headquarters or Service Provider site, or sent out a local PSTN gateway.

Remote Survivable Call Process Behavior

The following illustration shows the remote survivable call process behavior of the ROBO Oracle Enterprise Session Border Controller when connectivity fails to the Service Provider site (or headquarters site).



1. Phones register directly on remote site Oracle Enterprise Session Border Controller.
2. Phone-to-phone calls are proxied directly on remote site Net-Net ESD.
3. Phone-to-PSTN calls are routed by remote site Oracle Enterprise Session Border Controller to local PSTN gateway.

Entering Survivable Mode

Registration Behavior

When the Oracle Enterprise Session Border Controller enters Survivable Mode, it performs as follows for registrations:

For endpoints already Registered...	For new Registration requests... (either new endpoints or endpoints whose registration expires when in Survivable Mode)
the Oracle Enterprise Session Border Controller acts as the registrar of the local SIP phones by providing 200 OK responses to subsequent REGISTER refresh messages from endpoints in the Oracle Enterprise Session Border Controller's reg-cache for the duration of Survivable mode. This presumes that "registration-caching" has been enabled in the Oracle Enterprise Session Border Controller onfiguration.	the Oracle Enterprise Session Border Controller allows the new Registrations to be successful (without providing Authentication), incorporating them into the Oracle Enterprise Session Border Controller registration cache.

For endpoints already Registered...	For new Registration requests... (either new endpoints or endpoints whose registration expires when in Survivable Mode)
the Oracle Enterprise Session Border Controller lowers the "reg-expires" value to 30 seconds by default for all Registration Requests between the endpoints and the Oracle Enterprise Session Border Controller.	the Oracle Enterprise Session Border Controller lowers the "reg-expires" value to 30 seconds by default for all Registration Requests between the endpoints and the Oracle Enterprise Session Border Controller.

In Survivable Mode, the Oracle Enterprise Session Border Controller routes incoming INVITEs based on the lookup from the registration cache. If the entry is part of the registration cache, the INVITEs are routed depending on the contact information from the cache. If the entry is not part of the registration cache, local policy is used if there is any local policy configured on the Oracle Enterprise Session Border Controller. The prefix length in the Survivability configuration is taken into consideration when creating the extension for the phone number in the registration cache.

Call Processing Behavior

After the Oracle Enterprise Session Border Controller enters Survivable Mode, it performs as follows for call processing:

- Allows incoming sessions (either from an endpoint or an external PSTN gateway or alternate trunk) to be processed locally, based on its Registration cache.
- Locally handles multiple identities based on the registered P-Preferred-Identity (or via BroadSoft's proprietary mechanism).
- For session requests coming from local endpoint destined to non-local destinations, it routes to alternate PSTN gateways or SIP trunks, if configured.
- It performs registration cache (reg-cache) matching based on substrings of the received dialed digits (for example, a phone registers as sip:7813284545@acmepacket.com and a local user dials sip:4545@acmepacket.com).

Note: The Oracle Enterprise Session Border Controller allows extensions to be dialed based on it's multiple user identities (identified either by using P-Asserted-Identity or BroadSoft's proprietary mechanism.) For more information about Survivability when using the BroadSoft server, see *Remote Site Survivability with a BroadSoft Server*

Exiting Survivable Mode

Registration Behavior

When the Remote Oracle Enterprise Session Border Controller exits Survivable Mode, it performs as follows for registrations:

- It forwards all registration requests (new or refreshes) to the core data center (or headquarters) site. Note: All endpoints in the registration cache associated with that Registrar are invalidated.
- "The "expires" value is no longer set to 30 seconds by default. It takes the corresponding registration-refresh value based on the Oracle Enterprise Session Border Controller configuration.

Note: When the Oracle Enterprise Session Border Controller is in Normal Mode, it routes the incoming INVITEs to the registrar if the endpoint is part of the registration cache. If the endpoint is not part of the registration cache, the INVITEs are routed using the local policy if the local policy is configured on the Oracle Enterprise Session Border Controller. Otherwise, a 404 Not Found is returned.

Call Processing Behavior

When the Remote Net-Net ESD exits Survivable Mode, it performs as follows for Call Processing:

- It allows incoming sessions to be sent to the core data center (or headquarters) site for processing.
- Existing sessions remain connected until a user ends the session.

Remote Site Survivability with a BroadSoft Server

The Remote Site Survivability feature can be enabled on a Oracle Enterprise Session Border Controller to work in a network with a BroadSoft server by installing the Survivability Session Plug-in Language (SPL) on the Oracle Enterprise Session Border Controller called BroadsoftSurvivability.spl.

In this network configuration, the Oracle Enterprise Session Border Controller advertises Directory Numbers (DNs), extensions, and other aliases (in XML format) in the 200 OK response to the Registrar. When the Oracle Enterprise Session Border Controller enters Survivability mode, an indication is sent to the BroadSoft server (as an XML object) in the 200 OK response in the REGISTER or SUBSCRIBE message. The Oracle Enterprise Session Border Controller then sends originations to all Shared Call Appearance (SCA) destinations via the BroadSoft server.

The following illustration shows the IP Phone sending a Register messsage through the Oracle Enterprise Session Border Controller to the BroadSoft server, and a 200 OK response returned from the BroadSoft server (containing the applicable XML info) through the Oracle Enterprise Session Border Controller to the IP Phone.

In the event that the BroadSoft server is unavailable, the Oracle Enterprise Session Border Controller creates a location mapping entry, linking the parsed information (DNs, extensions, and aliases) to the location cache entry's Address of Record (AOR). This allows users to dial by extension even if the BroadSoft server is unavailable.

Remote Site Survivability Configuration

You must enable remote site survivability on the Oracle Enterprise Session Border Controller (E-SBC) and set the ping method for the session agent before the E-SBC can perform remote site survivability operations.

The process for configuring remote site survivability includes the following procedures.

1. Enable remote site survivability mode on the E-SBC.
2. Configure a ping method for the session agent to use to determine when the E-SBC is not responding.

Note: The system does not require a reboot after activating or modifying remote site survivability.

Configuring a Service Tag for an IP Interface

To configure a service-tag for an IP interface:

1. In Superuser mode, type configure terminal and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

2. Type session-router and press Enter.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

3. Type sip-interface and press Enter.

```
ACMEPACKET(session-router)# sip-interface
ACMEPACKET(sip-interface)#
```

4. service-tag—Enter a character string that identifies a group of session-agents for the current SIP interface. When Survivability is enabled, the Oracle Enterprise Session Border Controller monitors the health of the session-agents using this service-tag.

```
ACMEPACKET(sip-interface)# service-tag intf1
```

5. Type done and press Enter.

```
ACMEPACKET(sip-interface)# done
ACMEPACKET(sip-interface)#
```

6. Type exit and press Enter.

```
ACMEPACKET(sip-interface)# exit
ACMEPACKET(session-router)#
```

7. Save the configuration.

Configure Remote Site Survivability

You must enable remote site survivability on the Oracle Enterprise Session Border Controller (E-SBC) and set the parameters before the system can enter and exit survival mode.

Prerequisites

- Confirm that at least one session agent is configured.

To enable remote site survivability from the ACLI command line, do the following :

1. From the ACLI command line, access the survivability object, and press Enter.

```
ACMEPACKET(session-router)# survivability
ACMEPACKET(survivability)#
```

2. state. Type enabled, and press ENTER.
3. reg-expires. Type a value for the number of seconds that the Oracle Enterprise Session Border Controller waits before entering the remote site survivability mode, and press ENTER.
4. prefix-length. Type the maximum number of digits allowed for a phone extension, and press ENTER. Valid values are 0-10.
5. session-agent hostname. Type the session agent hostname or the session agent group name, and press ENTER.
6. Type done, and press Enter.
7. Type exit, and press Enter.
8. Save the configuration.

Post-requisites

- Configure a ping method for the session agent to use to determine when the E-SBC is not responding.

Configuring Service Health for a List of Service Tag

To configure the service health for a list of service tags:

1. Type service-health and press Enter.

```
ACMEPACKET(session-router)# service-health
ACMEPACKET(service-health)#
```

2. Type service-tag and press Enter.

```
ACMEPACKET(service-health)# service-tag-list
ACMEPACKET(serviceTag)#
```

3. service-tag-string—Enter a list of service tags (associated with IP interfaces) on which the Oracle Enterprise Session Border Controller checks the service health. Default is blank.

```
ACMEPACKET(serviceTag)# service-tag-string intf1,intf2,intf3
```

4. Type sa-health-profile and press Enter.

```
ACMEPACKET(serviceTag)# sa-health-profile
ACMEPACKET(sa-health-profile)#
```

5. session-agent-hostname—Enter the hostname of the session agent on which the Oracle Enterprise Session Border Controller monitors the service health.

```
ACMEPACKET(sa-health-profile)# session-agent-hostname SA1
ACMEPACKET(sa-health-profile)#
```

6. session-agent-health—Enter the health score that the Oracle Enterprise Session Border Controller uses to determine whether or not the health of the session-agent has decremented and gone out of service or incremented and came back into service. Valid values are 0 to 100 percent. Default is 100. For example, if this parameter is set to 100, and if the health score of the session-agent falls beneath 100 percent, Survivability mode begins (if

enabled). If the health of the session-agent comes back up to 100 percent, Survivability mode ends and the system returns to Normal mode.

Note: For cases where there are two session agents, each session agent could have a service health of 50.

```
ACMEPACKET(sa-health-profile)# session-agent-health 100
ACMEPACKET(sa-health-profile)#
```

7. Type done and press Enter.

```
ACMEPACKET(sa-service-health)# done
ACMEPACKET(sa-service-health)#
```

8. Type exit and press Enter.

```
ACMEPACKET(sa-service-health)# exit
ACMEPACKET(serviceTag)#
```

9. Type exit and press Enter.

```
ACMEPACKET(serviceTag)# exit
ACMEPACKET(service-health)#
```

10. Type exit and press Enter.

```
ACMEPACKET(service-health)# exit
ACMEPACKET(session-router)#
```

11. Save the configuration.

Configure the Ping Method for a Session Agent

Configure a ping method to confirm that the session agent is in service.

Use the session-agent object to configure the ping-method for a session-agent.

1. Access the session-agent object.

```
ACMEPACKET(session-router)# session-agent
ACMEPACKET(session-agent)#
```

2. ping-method—Type the SIP message/method to use to ping a session agent. Oracle recommends setting this value to OPTIONS.
3. ping-interval—Type the number of seconds between pings. The range is from 0-4294967295.
4. Type exit, and press Enter.
5. Save the configuration.

Example Remote Site Survivability Configuration

The following is an example of a Survivability mode configuration.

```
sip-interface
    service-tag        intf1
survivability
        state    enabled
        service-tag    intf1
        reg-expires    30
        prefix-length        4
service-health
    service-tag-list
        service-tag-string    intf1,intf2,intf3
        sa-health-profile
            session-agent-hostname    SA1
            session-agent-health    100
session-agent
    ping-method            BYE,ACK,OPTIONS,SUBSCRIBE,
                NOTIFY,INVITE,MESSAGE,INFO
```

Configuring Remote Site Survivability using the Web GUI

The Oracle Enterprise Session Border Controller Web GUI supports the configuration of Survivability.

Use the following procedure to configure Survivability.

Configure a Service Tag for an IP Interface

Configure a service tag to enable the Oracle Enterprise Session Border Controller to monitor the health of a group of session agents, when survivability is enabled.

- Confirm that survivability is enabled.
- Confirm that the system displays the Expert mode.

To configure a service-tag for an IP interface:

1. From the Web GUI, click **Configuration** > **session-router** > **sip-interface**.
2. On the Modify SIP Interface page, in the Service tag field, enter a character string that identifies a group of session-agents for the current SIP interface.
3. Click **OK**.
4. Save and activate the configuration.

Configure Remote Site Survivability

You must enable remote site survivability on the Oracle Enterprise Session Border Controller (E-SBC) and set the parameters before the system can enter and exit survival mode.

Before You Begin

- Confirm that at least one session agent is configured.
- Confirm that the system displays the Expert mode.

Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **survivability**.
2. At the bottom of the left pane, click **Show advanced**.
3. On the Add survivability page, do the following:

Attributes	Instructions
State	Select to enable Survivability.
Reg expires	Enter the number of seconds that the Oracle Enterprise Session Border Controller waits before entering the remote site survivability mode when the registration expires.
Prefix length	Enter the maximum number of digits allowed for a phone extension. Range: 0-10.
Session agent hostname	Select the agent hostname or the session agent group name from the drop down list.

4. Click **OK**.
5. Save and activate the configuration.

Next Steps

- Configure a ping method on the session agent. See "Configure a Session Agent."

Configure Service Health

To configure the service health for a list of service tags:

1. Select **session-router** > **service-health.**
2. In the service-tag-list window, click <Add>.
3. In the service-tag-string field, enter a list of service tags (associated with IP interfaces) on which the Oracle Enterprise Session Border Controller (E-SBC) checks the service health. Default is blank. For example, intf1, intf2, intf3.

4. In the sa-health-profile box, click <Add>.
5. In the session-agent-hostname field, enter the hostname of the session agent on which the E-SBC monitors the service health.
6. In the session-agent-health field, enter the health score that the E-SBC uses to determine whether or not the health of the session-agent has decremented and gone out of service or incremented and came back into service. Valid values are 0 to 100 percent. Default is 100. For example, if this parameter is set to 100, and if the health score of the session-agent falls beneath 100 percent, Survivability mode begins (if enabled). If the health of the session-agent comes back up to 100 percent, Survivability mode ends and the system returns to Normal mode.

   Note: For cases where there are two session agents, each session agent could have a service health of 50.

7. Click <OK>.
8. Save and activate the configuration.

Configure the Ping Method for a Session Agent

Configure a ping method to confirm that the session agent is in service.

Use the session-agent object to configure the ping-method for a session-agent.

1. Click **Configuration** > **session-router** > **session-agent.**
2. On the Modify Session Agent page, select the session-agent for which you want to configure the ping-method, and click **OK**.
3. In the **Ping method** field, enter the SIP message/method to use to ping a session agent. Oracle recommends setting this value to OPTIONS.
4. In the **Ping interval** field, enter the number of seconds between pings.
5. Click**OK**.
6. Save and activate the configuration.

Show Commands for Survivability

The Oracle Enterprise Session Border Controller allows you to use specific show commands to display statisitcal data about Survivability mode. Survivability mode data consists of Session Initiation Protocol (SIP) Request method statistics. You can initiate the show commands whether or not the Oracle Enterprise Session Border Controller is in Survivability mode. However, if you initiate the commands when the Oracle Enterprise Session Border Controller is in Normal mode, and Survivability mode was never initiated, the statistics display as zero (0).

This section describes the various show ACLI commands you can use to display statistics about the performance of Survivability on the Oracle Enterprise Session Border Controller.

Show Survivability Command

The show survivability command displays active and total statistics about the performance of Survivability mode over a period of time and for overall lifetime. This display also provides statistics related to SIP media events that occur while the Oracle Enterprise Session Border Controller is in Survivability mode.

Note: The statistics that display in the output for this command are also used in the Historical Data Recording (HDR) statistics for Survivability. For more information about HDR for Survivability, see *Historical Data Recording (HDR) for Survivability*.

The following example shows the output for the show survivability command.

Example

```
ACMEPACKET# show survivability
12:44:48-109
SIP Status                -- Period -- -------- Lifetime --------
                  Active     High   Total       Total  PerMax     High
Sessions               0        0       0           0       0        0
Subscriptions          0        0       0           0       0        0
Dialogs                0        0       0           0       0        0
```

```
CallID Map            0        0        0            0        0        0
Rejections            -        -        0            0        0
ReINVITEs             -        -        0            0        0
ReINV Suppress        -        -        0            0        0
Media Sessions        0        0        0            0        0        0
Media Pending         0        0        0            0        0        0
Client Trans          1        1        1          718        2        1
Server Trans          0        0        0            0        0        0
Resp Contexts         0        0        0            0        0        0
Saved Contexts        0        0        0            0        0        0
Sockets               2        2        0            2        2        2
Req Dropped           -        -        0            0        0
DNS Trans             0        0        0            0        0        0
DNS Sockets           0        0        0            0        0        0
DNS Results           0        0        0            0        0        0
Rejected Msgs         0        0        0            0        0        0
```

If Survivability mode was never initiated, the output shows values of zero (0) in all columns.

Output

The following table provides a description of this output.

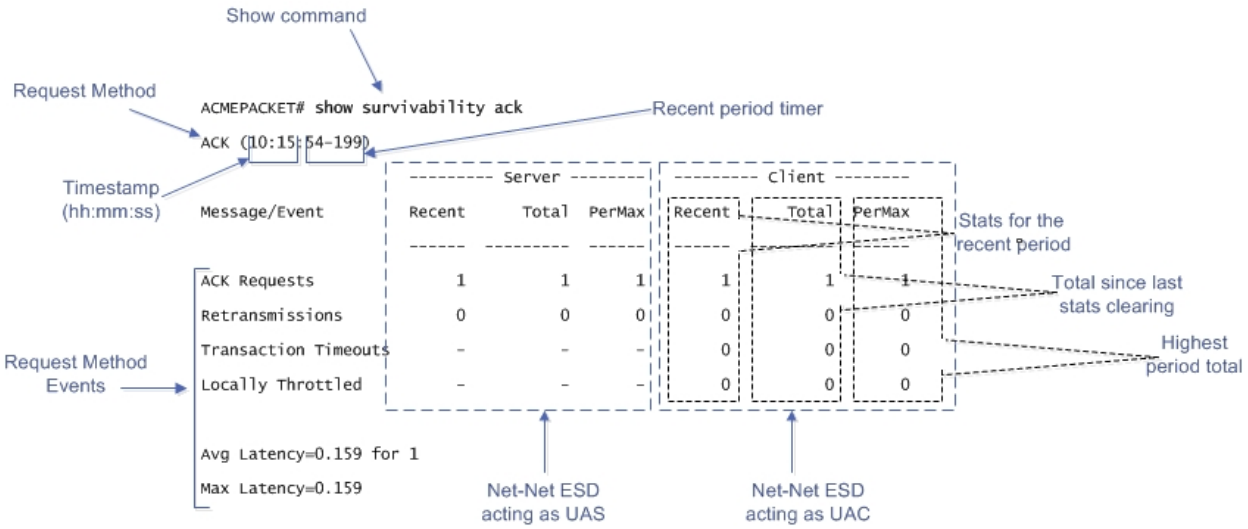
Event	Description
Sessions	Number of sessions established by INVITE and SUBSCRIBE messages during Survivability.
Subscriptions	Number of sessions established by SUBSCRIPTION during Survivability.
Dialogs	Number of end-to-end SIP signaling connections during Survivability.
CallID Map	Number of successful session header Call ID mappings during Survivability.
Rejections	Number of rejected INVITEs during Survivability.
ReINVITEs	Number of ReINVITEs during Survivability.
ReINV Suppress	Number of ReINVITEs that were suppressed during Survivability.
Media Sessions	Number of successful media sessions during Survivability.
Media Pending	Number of media sessions waiting to be established during Survivability.
Client Trans	Number of client transactions during Survivability.
Server Trans	Number of server transactions that have taken place on the Oracle Enterprise Session Border Controller during Survivability.
Resp Contexts	Number of response contexts during Survivability.
Saved Contexts	Number of saved contexts during Survivability.
Sockets	Number of SIP sockets during Survivability.
Req Dropped	Number of dropped requests during Survivability.
DNS Trans	Number of Domain Name System (DNS) transactions during Survivability.
DNS Sockets	Number of Domain Name System (DNS) sockets during Survivability.
DNS Results	Number of Domain Name System (DNS) results during Survivability.
Rejected Msgs	Number of rejected messages during Survivability.

Show Commands for Request Methods

The show survivability<method_name> command for SIP Request methods allow you to display specific statistical information about Request events that pass between the User Agent Server (UAS) and User Agent Client (UAC). Specific Request methods include:

SIP Request Method	Description
INVITE	Method used to request a session.
REGISTER	Method used to register the client with the server according to the address in the To header field.
BYE	Method used to terminate an established media session.
ACK	Method is used to acknowledge final responses to INVITE requests.
CANCEL	Method is used to terminate pending requests.
OPTIONS	Method used to query a user agent or server about its capabilities and discover its current availability.
REFER	Method used by a user agent to request another user agent to access a URI or URL resource.
SUBSCRIBE	Method used by a user agent to subscribe the device for the purpose of receiving notifications (via the NOTIFY method) about a particular event.
NOTIFY	Method used by a user agent to convey information about the occurrence of a particular event. A NOTIFY is always sent within a dialog, when a subscription exists between the subscriber and the notifier.
UPDATE	Method used to modify the state of a session without changing the state of the dialog,
PRACK	Method used to acknowledge receipt of reliably transported provisional responses. This is generated by a UAC.
MESSAGE	Method used to transport instant messages (IM) using SIP.
INFO	Method used to send information in the middle of a session that doesn't modify the session's state.
PUBLISH	Method used to publish an event state to the server.
OTHER	Method used

The following is an example of the show command output for an ACK Request.



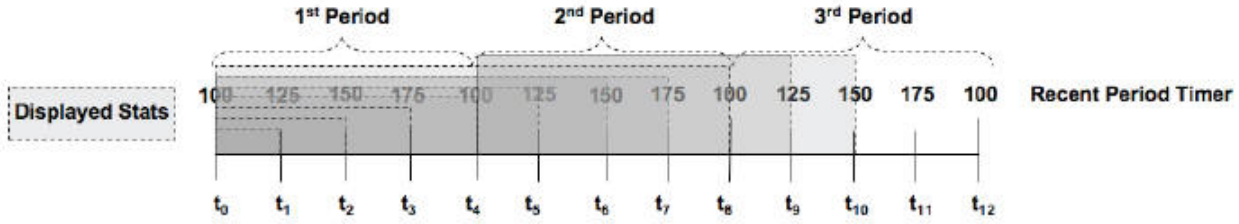
The example above provides a description for each area of the output. The Request method displays on the line directly under the command prompt (ACK in the above example), followed by the time stamp (hour:minute:second format), and then the recent period timer. The User Agent Server (UAS) data (when the Oracle Enterprise Session Border Controller is acting as a server) is listed in the middle of the display, and the User Agent Client (UAC) data (when the Oracle Enterprise Session Border Controller is acting as a client) is listed on the right side.

For both the UAS and UAC, the Recent column represents statistics for the recent period (the current period plus the last period). The Total column represents the total for a particular metric since the last stats clearing. Statistics are cleared either through the re-issue of the show survivability <method_name> command or on a reboot. The PerMax column represents the maximum for a given metric seen in any given individual (current) period.

Note: The "Recent" column represents the recent period, which includes statistics from the current and the last period, which is why that number may be higher than what displays in the PerMax column.

Recent Period Timer Operation

The Current period timer counts from 100 to 200 in one second increments as shown in the following illustration.



The statistics that display in the Recent column for any show survivability command reflects the appropriate behaviors for the associated value within the current period PLUS the last period (which constitutes a 100-200 second Recent period). This prevents the statistics from zeroing out between period transitions. So at time t4, in the display above, the statistics that display represent the last 100 seconds worth of behaviors (from the first period). The Recent Period statistics at time t6 represent the last 150 seconds of statistics (including 100 period 1). The Recent Period statistics at time t8 represent the last 100 seconds of statistics (including 100 from period 2).

The Recent period is the sum of the Active (current) period and the previous period.

SIP Request Method Examples

The following are examples of the show survivability <method_name> command. This command displays the recent and total Request events passed between the server and client when Survivability mode was enabled on the Oracle Enterprise Session Border Controller. This output also displays the maximum number of Request events that occurred during a current time period window of 100 seconds, when Survivability mode was enabled.

You can specify any SIP Request method for the <method_name>. The following example uses the INVITE SIP Request name.

Example 1

```
ACMEPACKET# show survivability invite
INVITE (10:15:44-189)
                        --------- Server --------   --------- Client --------
Message/Event           Recent      Total  PerMax   Recent      Total  PerMax
                        ------  ---------  ------   ------  ---------  ------
INVITE Requests              1          1       1        1          1       1
Retransmissions              0          0       0        0          0       0
100 Trying                   1          1       1        0          0       0
180 Ringing                  1          1       1        1          1       1
200 OK                       1          1       1        1          1       1
Response Retrans             0          0       0        0          0       0
Transaction Timeouts         -          -       -        0          0       0
Locally Throttled            -          -       -        0          0       0
Avg Latency=0.130 for 1
Max Latency=0.130
```

Example 2

The following example uses the REGISTER SIP Request name.

```
ACMEPACKET# show survivability register
REGISTER (09:55:26-150)
                        --------- Server --------   --------- Client --------
Message/Event           Recent      Total  PerMax   Recent      Total  PerMax
                        ------  ---------  ------   ------  ---------  ------
REGISTER Requests            4          4       4        4          4       4
Retransmissions              0          0       0        0          0       0
200 OK                       2          2       2        2          2       2
401 Unauthorized             2          2       2        2          2       2
Transaction Timeouts         -          -       -        0          0       0
Locally Throttled            -          -       -        0          0       0
Avg Latency=0.139 for 4
Max Latency=0.158
```

If Survivability mode was never initiated, the outputs show values of zero (0) in all columns.

show survivability commands

The following table describes the output for the “show survivability <method_name> command.

Message/Event	Description
INVITE Requests	Number of INVITE Request events that occurred between the server and client during Survivability mode.
Retransmissions	Number of retransmission of INVITE Request events that occurred during Survivability.
<Response Code>	Type and number of responses that occurred between the Client and Server during Surviability.
Transaction Timeouts	Number of INVITE Request event timeouts that occurred during Survivability.
Locally Throttled	Number of INVITE Request events that were locally throttled during Survivability. This is the number of INVITE Request events that were transmitted during the regulation (slowing down) of network traffic by the Oracle Enterprise Session Border Controller to minimize bandwidth congestion.

Message/Event	Description
Avg Latency	Average amount of time for INVITE Request events to travel in the time period window with the amount of events specified.
Max Latency	Maximum amount of time it took for INVITE Request events to travel in the time period window.

Show Commands for Session Agents Interfaces and Realms

The following show commands for Session Agents, interfaces and realms allow you to display recent and total statistics about the SIP methods used during Survivability mode:

- show survivability agents <hostname><method_name>
- show survivability interface <realm-id><method_name>
- show survivability realms <realm-id><method_name>

For each of these commands you can specify the SIP method name for which you want to display statistics. SIP method names include:

BYE	OPTIONS
UPDATE	SUBSCRIBE
CANCEL	NOTIFY
ACK	INFO
INVITE	MESSAGE
PRACK	PUBLISH
REFER	REGISTER
OTHER	

The output for these commands display recent and total number of SIP Requests that occurred for a session agent, interface, or realm during a current time period window of 100 seconds, when Survivability mode was enabled.

Note: To view the method names available, press the tab key after entering the command as shown in the following example.

```
ACMEPACKET# show survivability agents net192<tab>
ack           bye           cancel        info          invite        message
notify        options       other         prack         publish       refer
register      subscribe     update
```

The following examples show the output of the show survivability commands for agents, interface, and realms.

If Survivability mode was never initiated, the outputs show values of zero (0) in all columns.

Session Agents

```
ACMEPACKET# show survivability agents net192 refer
REFER (13:15:35-117)
                     --------- Server --------   --------- Client --------
Message/Event        Recent      Total  PerMax   Recent      Total  PerMax
                     ------  ---------  ------   ------  ---------  ------
REFER Requests            0          2       2        0          2       2
Retransmissions           0          0       0        0          0       0
202 Accepted              0          2       2        0          2       2
Transaction Timeouts      -          -       -        0          0       0
Locally Throttled         -          -       -        0          0       0
Avg Latency=0.000 for 0
Max Latency=0.000
```

Interface

```
ACMEPACKET# show survivability interface net192 refer
REFER (13:15:35-117)
                      --------- Server --------   --------- Client --------
Message/Event         Recent      Total  PerMax   Recent      Total  PerMax
                      ------  ---------  ------   ------  ---------  ------
REFER Requests             0          2       2        0          2       2
Retransmissions            0          0       0        0          0       0
202 Accepted               0          2       2        0          2       2
Transaction Timeouts       -          -       -        0          0       0
Locally Throttled          -          -       -        0          0       0
Avg Latency=0.000 for 0
Max Latency=0.000
```

Realms

```
ACMEPACKET# show survivability realms net192 refer
REFER (13:15:35-117)
                      --------- Server --------   --------- Client --------
Message/Event         Recent      Total  PerMax   Recent      Total  PerMax
                      ------  ---------  ------   ------  ---------  ------
REFER Requests             0          2       2        0          2       2
Retransmissions            0          0       0        0          0       0
202 Accepted               0          2       2        0          2       2
Transaction Timeouts       -          -       -        0          0       0
Locally Throttled          -          -       -        0          0       0
Avg Latency=0.000 for 0
Max Latency=0.000
```

Output

The following table describes the output for the above commands.

Message/Event	Description
<method_name> Requests	Number of the specified Request events that occurred between the server and client during Survivability mode.
Retransmissions	Number of retransmissions of specified Request message that occurred during Survivability.
<Response Code>	Type and number of responses that occurred between the Client and Server during Surviability.
Transaction Timeouts	Number of the specified Request event timeouts that occurred during Survivability.
Locally Throttled	Number of the specified Request events that were locally throttled during Survivability. This is the number of ACK Request events that were transmitted during the regulation (slowing down) of network traffic by the Oracle Enterprise Session Border Controller to minimize bandwidth congestion.
Avg Latency	Average amount of time for the specified Request events to travel in the time period window of 100 seconds, for the amount of events specified, during Survivability.
Max Latency	Maximum amount of time it took for the specified Request events to travel in the time period window of 100 seconds during Survivability.

Show Command for Survivability Status

The show survivability status command allows you to display the current status of Survivability mode on the Oracle Enterprise Session Border Controller. This command displays whether or not Survivability mode is enabled on an interface, and the date and time that Survivability mode was enabled.

The following is an example output of the show survivability status command.

Example

```
ACMEPACKET# show survivability status
Survivability
sip-interface  service-tag  state        start time       end time
-------------------------------------------------------------------
net192         test         enabled      Aug 15 12:53:01  -
net172         none         n/a          n/a              n/a
```

The following table describes the output for the above command.

Column	Description
sip-interface	Interface currently configured on the Net-Net ESD.
service-tag	Service tag that indicates the Session Agent Group (SAG) assigned to the interface on the Oracle Enterprise Session Border Controller.
state	Current Survivability state on the interface. Valid values are: enabled - Survivability is enabled on the interface disabled - Survivability is disabled on the interface n/a - Survivability does not configured on this interface.
start time	The date (MM:DD) and time (HH:MM:SS) that Survivability Mode became in-service on the interface.
end time	The date (MM:DD) and time (HH:MM:SS) that Survivability Mode became out-of-service on the interface. A - indicates that Survivability Mode is currently in-service and has not yet ended.

You can also display the current status of Survivability mode on a specific interface using the command, show survivability status <interface> where <interface> is the SIP interface name.

The following is an example output of the show survivability status <interface> cocmmand.

```
ACMEPACKET# show survivability status net192
Survivability
sip-interface  service-tag  state         start time       end time
-------------------------------------------------------------------
net192         test         enabled       Aug 15 12:53:01  -
```

Show Command for Service Health

When Survivability Mode is active on the Oracle Enterprise Session Border Controller, the system is able to detect any loss of connection (and subsequent re-connection) to the Enterprise's core data center based on a health score. The health score is the value that the Oracle Enterprise Session Border Controller uses to determine whether or not the health of the session-agent has decremented and gone out of service or incremented and came back into service.

You configure the service health at the ACLI path sessions-router->service-health ->service-tag-list->sa-health-profile->session-agent-health. Valid values are 0 to 100 percent. Default is 100. For example, if the session-agent-health parameter is set to 100, and if the health score of the session-agent falls beneath 100 percent, Survivability mode becomes in-service (if enabled). If the health of the session-agent comes back up to 100 percent, Survivability mode goes out of service, and the system returns to Normal mode.

For more information about service health in relation to Survivability on the Oracle Enterprise Session Border Controller, see *Survivability Health Score* .

You can display the current service-health of Survivability mode using the command show service-health at the root prompt.

If service-health on the Oracle Enterprise Session Border Controller is configured as follows:

```
service-health
        service-tag
                service-tag-string                      test
                sa-health-profile
                        session-agent-hostname     testAgent
                        session-agent-health     100
        last-modified-by                        admin@console
        last-modified-date                      2013-07-23 10:31:48
```

then the following are example outputs of the show service-health cocmmand when Survivability mode is in-service and out-of-service on the Oracle Enterprise Session Border Controller.

In-Service Example

```
ACMEPACKET# show service-health
service-tag      healthScore
test     100
```

Out-of-Service Example

```
ACMEPACKET# show service-health
service-tag      healthScore
test     0
```

Historical Data Recording (HDR) for Survivability

If the Oracle Enterprise Session Border Controller is configured to collect Historical Data Recording (HDR) statistics, statistics are collected on Survivability whether or not it is in-service.

HDR data consists of a “Group” with associated Group Statistics that apply to each group. HDR data comes from two sources:

- Simple Network Management Protocol (SNMP) Management Information Bases (MIBs)
- Oracle’s Command Line Interface (ACLI)

The Survivability data in the HDR outputs are taken from the ACLI. The following are the HDR Groups for survivability:

- survivability-sip-status
- survivability-sip-invites
- survivability-sip-register
- survivability-sip-errors

When the collector on the Oracle Enterprise Session Border Controller is enabled, these Groups and associated Group Statistics are included in the collection of data.

The following paragraphs provide a description of each Survivability Group and Group Statistic. Each Group table identifies the ACLI Show command for which it is associated.

Group survivability-sip-status

Description	Consists of statistics pertaining to the status of Survivability on the Oracle Enterprise Session Border Controller.
Group Statistics	*Sessions* *Subscriptions* *Dialogs* *CallID Maps* *Rejections* *ReINVITEs* *Media Sessions* *Media Pending* *Client Trans* *Server Trans* *Resp Contexts* *Saved Contexts* *Sockets* *Req Drops* *DNS Trans* *DNS Sockets* *DNS Results* *Session Rate* *Load Rate* *Active Subscriptions* *SubscriptionsPerMax* *Subscriptions High*
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Group Statistics

Sessions

Description	Total number of sessions established by INVITE and SUBSCRIBE messages during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295

ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Subscriptions

Description	Total number of sessions established by SUBSCRIPTION during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Dialogs

Description	Total number of end-to-end SIP signaling connections during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

CallID Maps

Description	Total number of successful session header Call ID mappings during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Rejections

Description	Total number of rejected INVITEs during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

ReINVITEs

Description	Total number of ReINVITEs during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Media Sessions

Description	Total number of successful media sessions during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Media Pending

Description	Total number of media sessions waiting to be established during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295

ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Client Trans

Description	Total number of client transactions during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Server Trans

Description	Total number of server transactions that have taken place on the Oracle Enterprise Session Border Controller during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Resp Contexts

Description	Total number of response contexts during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Saved Contexts

Description	Total number of saved contexts during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Sockets

Description	Total number of SIP sockets during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Req Drops

Description	Total number of dropped requests during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

DNS Trans

Description	Total number of Domain Name System (DNS) transactions during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295

ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

DNS Sockets

Description	Total number of Domain Name System (DNS) sockets during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

DNS Results

Description	Total number of Domain Name System (DNS) results during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Session Rate

Description	The rate, per second, of SIP invites allowed to or from the Oracle Enterprise Session Border Controller during the sliding window period, and during Survivability. The rate is computed every 10 seconds .
Type	period
Timer Value (seconds)	30
Range	0 to 4294967295
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Load Rate

Description	Average Central Processing Unit (CPU) utilization of the Oracle Enterprise Session Border Controller during the current window period, and during Survivability. The average is computed every 10 seconds unless the load-limit is configured in the SIPConfig record, in which case it is 5 seconds.
Type	period
Timer Value (seconds)	30
Range	0% to 100%
ACLI Show Command	show survivability
ACLI Parameter Mapping	For ACLI parameter mappings, see the table at *Show Survivability Command* .

Active Subscriptions

Description	Specifies the current global count of active SIP subscriptions during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability register
ACLI Parameter Mapping	For ACLI parameter mappings, see the command show sipd realms <realm_name> in the Net-Net SBC Historical Data Recording Resource Guide.

SubscriptionsPerMax

Description	Specifies the maximum global count of SIP subscriptions initiated during any 100 second period since the last SBC re-boot, and during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability register
ACLI Parameter Mapping	For ACLI parameter mappings, see the command show sipd realms <realm_name> in the Net-Net SBC Historical Data Recording Resource Guide.

Subscriptions High

Description	Specifies the maximum global count of active SIP subscriptions since the last SBC re-boot, and during Survivability.

Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability register
ACLI Parameter Mapping	For ACLI parameter mappings, see the command show sipd realms <realm_name> in the Net-Net SBC Historical Data Recording Resource Guide.

Group survivability-sip-invites

Description	**Consists of response statistics pertaining to INVITES during Survivability on the Oracle Enterprise Session Border Controller.**
Group Statistics	***INVITE Requests*** ***Retransmissions*** ***Response Codes*** **Each response code is next printed to the HDR file on a separate line. The format is <timestamp> <3-digit-code Description> <Total count> <Client total count>. See the above link to the Response Codes description table.** ***Response Retrans*** ***Transaction Timeouts*** ***Locally Throttled***
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Group Statistics

INVITE Requests

Description	Total number of INVITE requests during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Retransmissions

Description	Total number of retransmissions of INVITEs during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Response Codes

Description	Total number of a specific INVITE response codes that occurred during Survivability. Each of the response codes are as follows: 1xx --Informational: 100 Trying: This response is used to indicate the next node receives the request and stop the retransmission. This response is sent if there is delay in sending the final response more the 200ms. 180 Ringing: The response is generated if UA receives the INVITE and started the ringing. It may used to initiate local ring back. 181 Call is being Forwarded: This response is indication of call is being forwarded to different destination. 182 Call Queued: The called server is overloaded or temporary unavailable. the server sends this status code to queue the call. When server ready to take the call, it initiates appropriate final response. 183 Call Progress: This response may be used to send extra information for a call which is still being set up. 2xx—Successful Responses 200 OK: Indicates the request was successful. 202 Accepted: Indicates that the request has been accepted for processing, but the processing has not been completed. 3xx—Redirection Response 301 Moved Permanently: The original Request-URI is no longer valid, the new address is given in the Contact header field, and the client should update any records of the original Request-URI with the new value. 302 Moved Temporarily: The client should try at the address in the Contact field. If an Expires field is present, the client may cache the result for that period of time. 305 Use Proxy: The Contact field details a proxy that must be used to access the requested destination. 380 Alternative Service: The call failed, but alternatives are detailed in the message body. 4xx—Client Failure Responses 400 Bad Request: The request could not be understood due to malformed syntax.

	401 Unauthorized: The request requires user authentication. This response is issued by UASs and registrars. 403 Forbidden: The server understood the request, but is refusing to fulfill it 404 Not Found: The server has definitive information that the user does not exist at the domain specified in the Request-URI. This status is also returned if the domain in the Request-URI does not match any of the domains handled by the recipient of the request. 405 Method Not Allowed: The method specified in the Request-Line is understood, but not allowed for the address identified by the Request-URI. 406 Not Acceptable: The resource identified by the request is only capable of generating response entities that have content characteristics but not acceptable according to the Accept header field sent in the request. 407 Proxy Authentication Required: The request requires user authentication. This response is issued by proxys
	4xx—Client Failure Responses (continued) 408 Request Timed Out: Couldn't find the user in time. 415 Unsupported Media Type: Request body in a format not supported. 420 Bad Extension: Bad SIP Protocol Extension used, not understood by the server. 421 Extension Required: The server needs a specific extension not listed in the Supported header. 422 Session Interval Too Small: The received request contains a Session-Expires header field with a duration below the minimum timer. 423 Interval Too Brief: Expiration time of the resource is too short. 480 Temporarily Unavailable: Callee currently unavailable. 481 Call/Transaction Does Not Exist: Server received a request that does not match any dialog or transaction. 482 Loop Detected: Server has detected a loop. 483 Too Many Hops: Max-Forwards header has reached the value '0'. 484 Address Incomplete: Request-URI incomplete. 485 Ambiguous: Request-URI is ambiguous. 486 Busy Here: Callee is busy. 487 Request Terminated: Request has terminated by bye or cancel. 488 Not Acceptable Here: Some aspects of the session description of the Request-URI is not acceptable. 489 Bad Event: The server did not understand an event package specified in an Event header field. 491 Request Pending: Server has some pending request from the same dialog.
	5xx—Server Failure Responses 500 Server Internal Error: The server could not fulfill the request due to some unexpected condition. 501 Not Implemented: The server does not have the ability to fulfill the request, such as because it does not recognize the request method. (Compare with 405 Method Not Allowed, where the server recognizes the method but does not allow or support it.)

	502 Bad Gateway: The server is acting as a gateway or proxy, and received an invalid response from a downstream server while attempting to fulfill the request. 503 Service Unavailable: The server is undergoing maintenance or is temporarily overloaded and so cannot process the request. A "Retry-After" header field may specify when the client may re attempt its request. 504 Server Time-out: The server attempted to access another server in attempting to process the request, and did not receive a prompt response. 513 Message Too Large: The request message length is longer than the server can process. 580 Precondition Failure: The server is unable or unwilling to meet some constraints specified in the offer. 6xx—Global Failure Responses 600 Busy Everywhere: All possible destinations are busy. Unlike the 486 response, this response indicates the destination knows there are no alternative destinations (such as a voicemail server) able to accept the call. 603 Decline: The destination does not wish to participate in the call, or cannot do so, and additionally the client knows there are no alternative destinations (such as a voicemail server) willing to accept the call. 604 Does Not Exist Anywhere: The server has authoritative information that the requested user does not exist anywhere. 606 Not Acceptable: The user's agent was contacted successfully but some aspects of the session description such as the requested media, bandwidth, or addressing style were not acceptable.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Response Retrans

Description	Total number of INVITE response retransmissions during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Transaction Timeouts

Description	Total number of INVITE request transaction timeouts during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Locally Throttled

Description	Total number of INVITE requests locally throttled during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Group survivability-sip-register

Description	**Consists of response statistics pertaining to REGISTRATIONS during Survivability on the Oracle Enterprise Session Border Controller.**
Group Statistics	***REGISTRATION Requests*** ***Retransmissions*** ***Response Retrans*** ***Transaction Timeouts*** ***Locally Throttled***
ACLI Show Command	show survivability register
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability register” at *SIP Request Method Examples* .

Group Statistics

REGISTRATION Requests

Description	Total number of Register requests sent between the client and server during Surivability.

Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability register
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability register” at *SIP Request Method Examples* .

Retransmissions

Description	Total number of Register retransmissions that ocurred during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability register
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability register” at *SIP Request Method Examples* .

Response Retrans

Description	Total number of Register response retransmissions during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Transaction Timeouts

Description	Total number of Register request transaction timeouts during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite

ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Locally Throttled

Description	Total number of Register requests locally throttled during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability invite
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability invite” at *SIP Request Method Examples* .

Group: survivability-sip-errors

Description	**Consists of response statistics pertaining to REGISTRATIONS during Survivability on the Oracle Enterprise Session Border Controller.**
Group Statistics	***SDP Offer Errors*** ***SDP Answer Errors*** ***Drop Media Errors*** ***Transaction Errors*** ***Application Errors*** ***Media Exp Events*** ***Early Media Exps*** ***Exp Media Drops*** ***Expired Sessions*** ***Multiple OK Drops*** ***Multiple OK Terms*** ***Media Failure Drops*** ***Non-ACK 2xx Drops*** ***Invalid Requests*** ***Invalid Responses*** ***Invalid Messages*** ***CAC Session Drop*** ***CAC BW Drop***
ACLI Show Command	show survivability errors

Description	Consists of response statistics pertaining to REGISTRATIONS during Survivability on the Oracle Enterprise Session Border Controller.
Group Statistics	***SDP Offer Errors*** ***SDP Answer Errors*** ***Drop Media Errors*** ***Transaction Errors*** ***Application Errors*** ***Media Exp Events*** ***Early Media Exps*** ***Exp Media Drops*** ***Expired Sessions*** ***Multiple OK Drops*** ***Multiple OK Terms*** ***Media Failure Drops*** ***Non-ACK 2xx Drops*** ***Invalid Requests*** ***Invalid Responses*** ***Invalid Messages*** ***CAC Session Drop*** ***CAC BW Drop***
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Group Statistics

SDP Offer Errors

Description	Total number of errors encountered during Survivability, in setting up the media session for a session description in a SIP request or response which is a Session Description Protocol (SDP) Offer in the Offer/Answer model (RFC 3264).
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

SDP Answer Errors

Description	Total number of errors encountered during Survivability, in setting up the media session for a session description in a SIP request or response which is a Session Description Protocol (SDP) Answer in the Offer/Answer model (RFC 3264)
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Drop Media Errors

Description	Total number of errors encountered during Survivability, in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction, or b) a BYE transaction received from one of the participants in a dialog/session, or c) a BYE initiated by the Net-Net SD due to a timeout notification from the Middlebox Control Daemon (MBCD).
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Transaction Errors

Description	Total number of errors encountered during Survivability when processing SIP client transactions associated with setting up or tearing down of the media session.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Application Errors

Description	Total number of miscellaneous errors in the SIP application that are otherwise uncategorized during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples*.

Media Exp Events

Description	Total number of flow timer expiration notifications received from the Middlebox Control Daemon (MBCD) during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Early Media Exps

Description	Total number of flow timer expiration notifications received for media sessions that were not completely set up due to an incomplete or pending INVITE transaction during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Exp Media Drops

Description	Total number of flow timer expiration notifications from the Middlebox Control Daemon (MBCD) that resulted in the termination of the dialog/session by the SIP application during Survivability.

Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Expired Sessions

Description	Total number of sessions terminated due to the session timer expiring during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Multiple OK Drops

Description	Total number of dialogs terminated upon reception of a 200 OK response from multiple User Agent Servers (UASs) for a given INVITE transaction that was forked by a downstream proxy during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Multiple OK Terms

Description	Total number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Oracle Enterprise Session Border Controller during Survivability.
Type	counter
Timer Value (seconds)	N/A

Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Media Failure Drops

Description	Total number of dialogs terminated due to a failure in establishing the media session during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Non-ACK 2xx Drops

Description	Total number of sessions terminated because an ACK was not received for a 2xx response during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Invalid Requests

Description	Total number of invalid requests (for example, an unsupported header was received) during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors

ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Invalid Responses

Description	Total number of invalid responses (for example, no Via header in response) during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

Invalid Messages

Description	Total number of messages dropped due to parse failure during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

CAC Session Drop

Description	Total number of call admission control (CAC) session setup failures during Survivability.
Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

CAC BW Drop

Description	Total number of call admission control (CAC) session setup failures due to insufficient bandwidth (BW) during Survivability.

Type	counter
Timer Value (seconds)	N/A
Range	0 to 4294967295
ACLI Show Command	show survivability errors
ACLI Parameter Mapping	For ACLI parameter mappings, see the command “show survivability errors” at *SIP Request Method Examples* .

SNMP Trap for Survivability

A Oracle Enterprise Session Border Controller MIB contains objects of management data, and also information about Simple Network Management Protocol (SNMP) traps, which enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. When an element sends a TRAP packet, it can include an Object Identifier (OID) and value information (bindings) to clarify the event. For more information about SNMP on the Oracle Enterprise Session Border Controller, see the Net-Net 4000 MIB Reference Guide.

The Oracle Enterprise Session Border Controller triggers an Enterprise SNMP trap when a SIP interface goes in or out of Survivability mode. This trap is called:

- snmp_survivability_mode_trap_send

This trap has been added to the SIP application MIB called ap-sip.mib. The trap information is as follows in this MIB:

```
apSipSurvivabilityNotif                OBJECT IDENTIFIER ::=
{ apSipNotificationObjects 2 }
apSipSurvivabilityNotifObjects      OBJECT IDENTIFIER ::=
{ apSipSurvivabilityNotif 1 }
apSipSurvivabilityNotifPrefix       OBJECT IDENTIFIER ::=
{ apSipSurvivabilityNotif 2 }
apSipSurvivabilityNotifications     OBJECT IDENTIFIER ::=
{ apSipSurvivabilityNotifPrefix 0 }
apSipSurvivabilityModeEnter     NOTIFICATION-TYPE
    OBJECTS    { apSysMgmtSipInterfaceRealmName,
apSysMgmtSipInterfaceIP  }
    STATUS        current
    DESCRIPTION
    " The trap will be generated when SIP interface enters Survivability
Mode."
    ::= { apSipSurvivabilityNotifications 1 }
apSipSurvivabilityModeExit         NOTIFICATION-TYPE
    OBJECTS    { apSysMgmtSipInterfaceRealmName,
         apSysMgmtSipInterfaceIP  }
    STATUS        current
    DESCRIPTION
        " The trap will be generated when SIP interface exits Survivability
Mode and resumes normal operation."
    ::= { apSipSurvivabilityNotifications 2 }
apSipSurvivabilityNotificationsGroup     NOTIFICATION-GROUP
        NOTIFICATIONS {apSipSurvivabilityModeEnter,
            apSipSurvivabilityModeExit  }
        STATUS      current
        DESCRIPTION
        "Traps to monitor  SIP interface Survivability feature."
        ::= { apSipNotificationGroups  2 }
```

Note: The apSysMgmtSipInterfaceRealmName and apSysMgmtSipInterfaceIP objects are imported strings defined in ap-smgmt.mib.

When this trap is generated, it contains the following information:

realmname	Realm name of the SIP interface
ipaddr	IP address of the SIP interface
mode	Specifies whether or not the SIP interface is in survivability mode. Values included with the trap are: 0 - SIP interface is OK. It is not in Survivability mode. 1 - SIP interface is in Survivability mode.

The following table identifies the Survivability OBJECT IDENTIFIERS in the Oracle MIB that the Oracle Enterprise Session Border Controller supports.

Trap Name: OID Number	Description
apSipSurvivabilityNotificationsGroupCap: 1.3.6.1.4.1.9148.2.1.21.3	Specifies the capability of the Oracle Enterprise Session Border Controller to notify the Agent regarding Survivability on the SIP interface.
apSipSurvivabilityNotif 1.3.6.1.4.1.9148.3.15.2.2	N/A
apSipSurvivabilityNotifObjects 1.3.6.1.4.1.9148.3.15.2.2.1	N/A
apSipSurvivabilityNotifPrefix 1.3.6.1.4.1.9148.3.15.2.2.2	N/A
apSipSurvivabilityNotifications 1.3.6.1.4.1.9148.3.15.2.2.2.0	N/A
apSipSurvivabilityModeEnter 1.3.6.1.4.1.9148.3.15.2.2.2.0.1	Specifies that the SIP interface has entered Survivability mode.
apSipSurvivabilityModeExit 1.3.6.1.4.1.9148.3.15.2.2.2.0.2	Specifies that the SIP interface has exited Survivability mode and resumed normal operation.
apSipSurvivabilityNotificationsGroup 1.3.6.1.4.1.9148.3.15.3.2.2	Specifies the notification from the Oracle Enterprise Session Border Controller to the Agent regarding Survivability on the SIP interface.

Survivability Alarms and Logging

All survivability debug information and messages are logged to the serviceHealth.log. When a SIP interface enters Survivability Mode, a MAJOR alarm is raised. The alarm message contains the SIP interface's IP address and realm ID on which it resides. The following is an example of the alarm.

Survivability Alarm Example

```
ID    Task    Severity    First Occurred    Last Occurred
3145745    776175088    4         2013-08-20 10:19:35     2013-08-20 10:19:35
Count    Description
1    SIP interface ip=172.16.38.17 realm-id=core running in Survivability Mode
```

ELIN Gateway Support

An Emergency Location Identification Number (ELIN)-capable gateway supports connections to a qualified E911 service provider. As such, they support PSTN-based E911 functions, including user call back if there is a disconnect. In addition, enterprises often deploy ELIN numbers based on physical location, providing them with the ability to locate the physical source of a 911 call. And by purchasing multiple ELINs, the enterprise can more easily support multiple, simultaneous E911 calls.

Typically, an enterprise purchases multiple ELIN numbers for use within their environment. ELIN gateways replace VoIP extension URIs with ELIN numbers and maintain these mappings. If the emergency service were to reply to a VoIP URI, the reply would be delayed or fail. An ELIN gateway, however, can use its mapping to translate the ELIN number back to the VoIP extension from within the enterprise session network. The gateway can, therefore, immediately forward the call back to the original client.

The Oracle Enterprise Session Border Controller now supports E911 ELIN for Lync-enabled Enterprises using the ELIN_Gateway SPL option. You enable this option by setting it within the global SPL configuration. The Oracle Enterprise Session Border Controller supports up to 300 ELIN numbers simultaneously, but can reuse numbers allowing the maximum number of emergency calls to be larger.

How the Emergency Location Identification Number (ELIN) SPL Works

When a Lync client places a 911 emergency call through a mediation server to a Oracle Enterprise Session Border Controller, the server indicates the emergency status in the priority field and provides a list of ELIN numbers. When the ELIN gateway module is enabled, the Oracle Enterprise Session Border Controller intelligently selects a particular ELIN number and uses it as the ANI in the “From” field SIP URI in the outgoing INVITE.

The Oracle Enterprise Session Border Controller preserves the mapping of used ELIN numbers in an internal table. This table includes the ELIN number, the caller (VoIP extension), the “in-use” count, and a timer field. The Oracle Enterprise Session Border Controller retains these mappings for a configurable time period ranging from 30 to 60 minutes after the call is terminated. The default is 30 minutes. When the timer expires, the entry is purged from the table. The timer field shows the time of day that the timer started.

You can view the current ELIN table at any time using the ACLI command spl show sip elins.

After the Lync client call is disconnected, the 911 service may call back using the number provided in the “From” field of the original INVITE. This presence of this number in its ELIN number table allows the Oracle Enterprise Session Border Controller to route the call back to the original caller.

Number Reuse

The Oracle Enterprise Session Border Controller can use an ELIN number for multiple calls. When a call that requires an ELIN mapping arrives at the Oracle Enterprise Session Border Controller, it checks to see if the numbers presented by the mediation server are in use. If a number is not in use, it simply uses that number. A number is not in use if it is not in the table or its “used count” is 0. An entry’s used count is zero when its not in use and its purge timer has not yet expired.

If all numbers are in use, the Oracle Enterprise Session Border Controller employs a means of reusing a number, incrementing its used count for each additional call. The selection process proceeds in the following order:

1. If the “caller” is in the ELIN table, the Oracle Enterprise Session Border Controller selects that mapping.
2. The Oracle Enterprise Session Border Controller selects the number with the lowest “ELIN count”.

If an ELIN number is used by multiple calls, it maps callback attempts to that ELIN number to the client that was last associated with the number.

Error Handling

Lync mediation servers always expect 503 “Service Unavailable” as an error message to a failed ELIN call. There is a variety of error messages that the network may send back when a call fails. For the purposes of Lync support, the Net-Net ESD sends 503 “Service Unavailable” to indicate call failure to a mediation server, regardless of the error it receives.

Configure the Emergency Location Identification Number (ELIN) Gateway Option

The ELIN-Gateway option must be configured at the global level under spl-config or by way of the Web GUI. The ELIN-Gateway option is not recognized in the session-agent, realm-config, or sip-interface.

Determine the preferred length of time to retain ELIN mappings within the Oracle Enterprise Session Border Controller. The range is from 30 to 60 minutes. The default is 30 minutes.

To configure the ELIN Gateway option:

1. In Superuser mode, type configure terminal and press <Enter>.
   ACMEPACKET# configure terminal
2. Type system, and press <Enter>.

```
ACMEPACKET(configure)# system
ACMEPACKET(system)#
```

3. Type spl-config, and press <Enter>.

```
ACMEPACKET(configure)# spl-config
ACMEPACKET(spl-config)#
```

4. Type spl-options +Extension-Headers="<value>" where <value> is the additional header information to store, and press <Enter>. The default behavior stores only the Request-URI and realm-id.

```
ACMEPACKET(spl-config)#spl-options +Elin-Gateway=60
```

5. Type done to save your work.

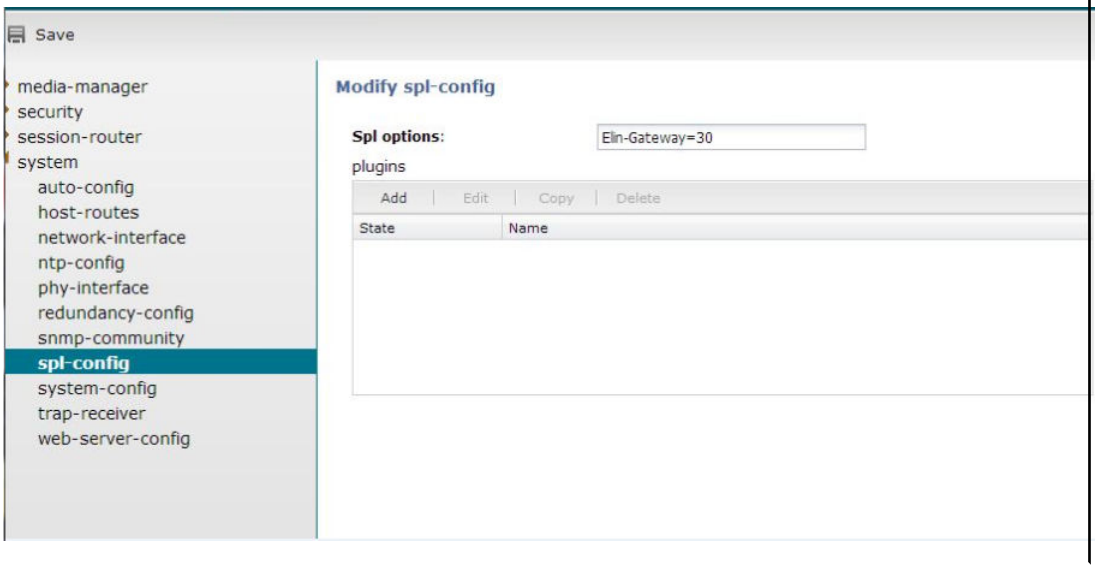
The following is an example of an Elin_Gateway SPL configuration:

```
system
    spl-config
        spl-options          Elin-Gateway=60
```

The following is an example of the ACLI command spl show sip elins.

```
ACMEPACKET#show sip elins
Elin:1111442231
Count:0 From:5555221134 Time:1380490337.8292
--------------
Elin:2222882232
Count:0 From:6666111234 Time:1380490770.4083
```

To configure the ELIN-Gateway option using the Web GUI, select spl-config, add a config, and save.



Avaya Session Manager (SM) Redundancy

To support redundancy in Avaya SM deployments, the Oracle Enterprise Session Border Controller can use the mechanisms for maintaining multiple connections defined in RFC 5626. In an Avaya SM deployment, this scenario is referred to as Dual Registration.

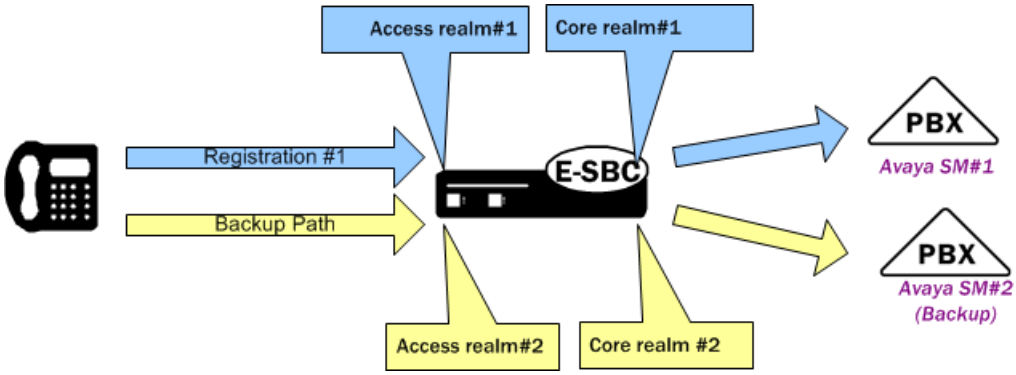
RFC 5626 specifies a method of maintaining connections between UAs and proxies, and outlines a general means for UAs to establish connection redundancy. The Oracle Enterprise Session Border Controller can use RFC 5626 specifically for redundancy in Avaya SM Dual Registration deployments. Such a deployment allows the network to continue to provide service by way of a redundant Avaya SM, when the primary Avaya SM stops responding.

Oracle Enterprise Session Border Controller configuration requires adding the rfc 5626 SPL option. In addition to adding the SPL option, the Oracle Enterprise Session Border Controller configuration design separates Avaya SMs and UA traffic by way of using realms.

How Avaya Session Manager (SM) Redundancy Works

To support Avaya SM redundancy, you configure multiple realms on the access side and the core side of the Oracle Enterprise Session Border Controller. These realms create the primary path and backup path for accessing a redundant Avaya SM.

Consider two Avaya SMs deployed for redundancy. You configure a core side realm for each Avaya SM and you configure two access side realms. Each access side realm is associated with the applicable core side realm, to which a UA sends registration messaging. The following illustration shows this configuration.



The operational scenario consists of the Avaya SM infrastructure providing configuration information to the UAs. The information includes the 2 proxy addresses, targeting the Oracle Enterprise Session Border Controller access-side interfaces. The UA knows which proxy is for the primary path, and sends initial REGISTER messages by way of that path. While the primary Avaya SM is up, the UA manages all registration exchanges, including refresh and re-register procedures, on the primary path. If the primary Avaya SM stops responding, the infrastructure informs the UA that it needs to register with the backup Avaya SM. The UA registers with the backup Avaya SM using the backup path.

The UA, by way of configuration, populates the backup registration and subsequent registration messages so that the Avaya SM infrastructure knows that the registrations are for the same UA. Key elements of the messaging and their use by the Avaya dual registration infrastructure include:

- reg-id - A contact header field parameter value that specifies individual registrations. UAs use unique reg-id values to specify registrations for individual flows.
- instance-id (+sip.instance) - A URN within the contact header that specifies a UA instance. UAs use the same Instance ID information in REGISTER exchanges to indicate that the registrations belong to the same UA.
- Route - The target proxy for the message. The UA uses route headers to define the separate paths to the Oracle Enterprise Session Border Controller.

The Avaya SM uses reg-id in conjunction with instance-ID to manage dual registrations. By keeping instance-ID the same and sending a new reg-id, the infrastructure recognizes that a redundant registration was generated because a session manager switchover occurred.

Normally, multiple reg-ids based on a single contact would trigger a "move" procedure. The presence of a single instance-ID tells the infrastructure that the reg-id change does not indicate a move.

The following example REGISTERs depict the population of these elements for the purposes of an Avaya dual registration scenario.

```
 REGISTER sip:example.com SIP/2.0
Via: SIP/2.0/TCP 192.0.2.2;branch=z9hG4bK-bad0ce-11-1036
Max-Forwards: 70
From: Bob <sip:bob@example.com>;tag=d879h76
To: Bob <sip:bob@example.com>
Call-ID: 8921348ju72je840.204
Supported: path, outbound
Route: <sip:ep1.example.com;lr>
CSeq: 1 REGISTER Supported: path, outbound
Contact: <sip:line1@192.0.2.2;transport=tcp>; reg-id=1;
;+sip.instance="<urn:uuid:00000000-0000-1000-8000-000A95A0E128>" Content-
Length: 0
```

Note the following redundant registration. The registration includes a different route header for the second Oracle Enterprise Session Border Controller realm. It also includes a new reg-id and the same instance-ID.

```
 REGISTER sip:example.com SIP/2.0
Via: SIP/2.0/TCP 192.0.2.2;branch=z9hG4bK-bad0ce-11-1036
Max-Forwards: 70
From: Bob <sip:bob@example.com>;tag=d879h76
To: Bob <sip:bob@example.com>
Call-ID: 8921348ju72je840.204
Supported: path, outbound
Route: <sip:ep2.example.com;lr>
CSeq: 1 REGISTER Supported: path, outbound
Contact: <sip:line1@192.0.2.2;transport=tcp>; reg-id=2;
;+sip.instance="<urn:uuid:00000000-0000-1000-8000-000A95A0E128>" Content-
Length: 0
```

Registration Caching

Enabling the RFC 5626 SPL option causes the Oracle Enterprise Session Border Controller to store a single, entire contact header in its registration cache for the AOR. When an Avaya SM switchover occurs, the Oracle Enterprise Session Border Controller updates the AOR by replacing the contact header with the new one. The Oracle Enterprise Session Border Controller does not store more than one contact per AOR. The Oracle Enterprise Session Border Controller establishes a flow with only the active Avaya SM.

Configure Avaya Session Manager (SM) Redundancy

The rfc5636 SPL option allows the Oracle Enterprise Session Border Controller to support Avaya Dual Registration for establishing redundant UA registration.

The rfc5626 option must be configured at the global level under spl-config or using the Web GUI. The rfc5626 option is not recognized in the session-agent, realm-config, or sip-interface.

To configure the rfc5626 option:

1. In Superuser mode, type configure terminal and press <Enter>.
   ACMEPACKET# configure terminal
2. Type system and press <Enter>.

   ```
   ACMEPACKET(configure)# system
   ACMEPACKET(system)#
   ```
3. Type system and press <Enter>.

   ```
   ACMEPACKET(system)# spl-config
   ACMEPACKET(spl-config)#
   ```
4. Type rfc5626 and press <Enter>.

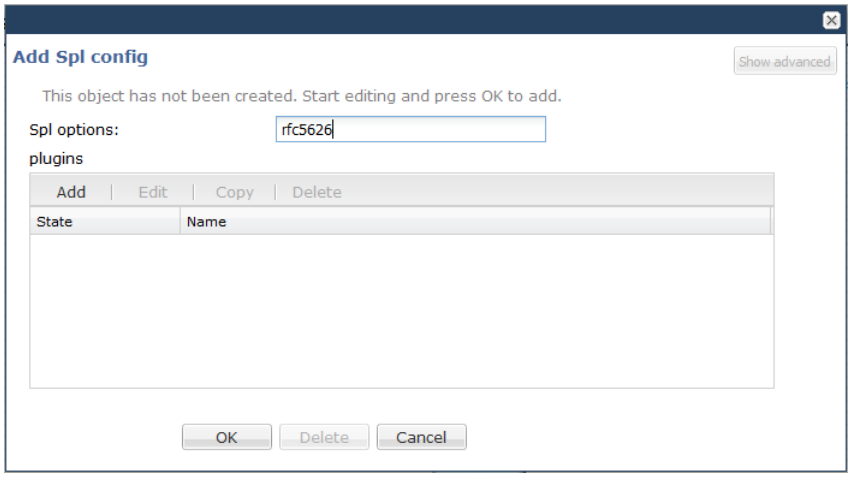
   ```
   ACMEPACKET(spl-config)# rfc5626
   ACMEPACKET(spl-config)#
   ```

5. Type done to save your work.
6. Save and Activate your configuration.

The following example shows an rfc5626 SPL configuration:

```
system
    spl-config
        spl-options          rfc5626
```

You can also configure the rfc5626 option using the Web GUI. The procedure consists of simply opening the spl-config dialog, adding the SPL option, then saving and activating.



P-Certificate-Subject-Common-Name to REGISTER Messages

Most Enterprises use revocation servers to authenticate certificates when the UE registers with the Oracle Enterprise Session Border Controller. However, for high security Enterprises (such as government organizations), a stolen UE (such as a cell phone) can have a certificate installed, and before that certificate is revoked from the server, the UE could register with the Oracle Enterprise Session Border Controller and then login to the system.

Release E-C[xz]6.4.0 M2 includes a Oracle Enterprise Session Border Controller feature that allows you to enable or disable the addition of a User certificate in the incoming REGISTER message header. This provides an additional layer of security when the UE registers with the Oracle Enterprise Session Border Controller. When this feature is enabled, the individual user certificate must match the user's identity during Registration.

You can enable or disable this feature using the "verify-certificate-info-register" parameter under the existing enforcement-profile object in session-router. in the ACLI. When enabled, and a REGISTER message is encountered, the Oracle Enterprise Session Border Controller adds the User certificate info to the message header. The header is then used in validating the Request-URI Based on certificate Information.

Configure the P-Certificate-Subject-Common-Name From the ACLI

Use the following procedure to configure the P-Certificate-Subject-Common-Name.

To configure the P-Certificate-Subject-Common-Name:

1. In Superuser mode, type configure terminal, and press Enter.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)#
```

2. Type session-router, and press Enter.

```
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)#
```

3. Type enforcement-profile, and press Enter.

```
ACMEPACKET(session-router)# enforcement-profile
ACMEPACKET(enforcement-profile)#
```

4. add-certificate-info—Enter sub-common name for the certificate attribute names to enable TLS certificate information caching, and for the inserting of cached certificate information into customized SIP INVITEs. Default is blank. Valid values are:
   - sub-common name
   - sub-alt-name-DNS
5. certificate-ruri-check—Enable this parameter if you want your Oracle Enterprise Session Border Controller to cache TLS certificate information and use it to validate Request-URIs. Enabling this parameter allows the Net-Net ESD to cache the TLS certificate information in a customized SIP INVITE. Default is disabled. Valid values are:
   - enabled
   - disabled
6. verify-certificate-info-register —Select whether or not to allow the Oracle Enterprise Session Border Controller to add certificate information to the header of a REGISTER message for verifying a ruri against certificate attributes. Default is disabled. Valid values are:
   - enabled
   - disabled
7. Type done, and press Enter.

```
ACMEPACKET(enforcement-profile)# done
ACMEPACKET(enforcement-profile)#
```

8. Type exit, and press Enter.

```
ACMEPACKET(enforcement-profile)# exit
ACMEPACKET(session-router)#
```

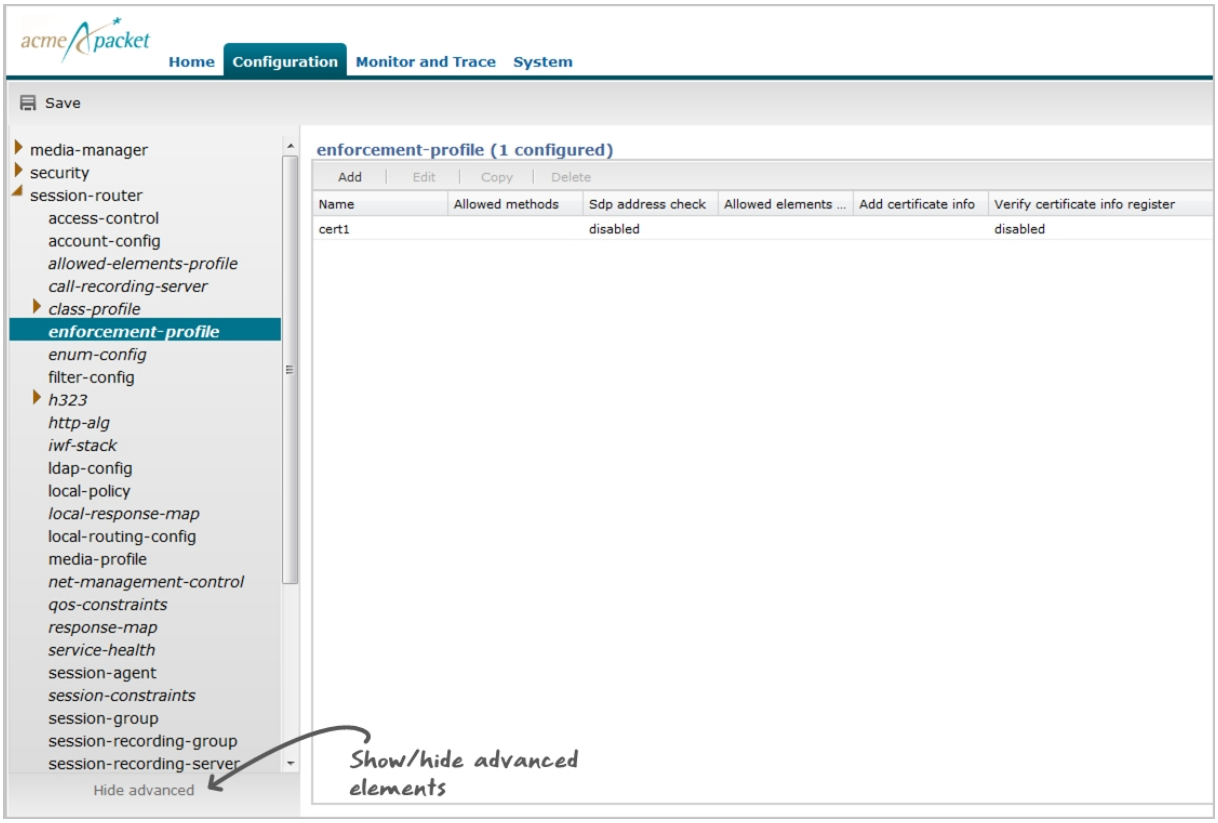
9. Save the configuration.

Configure the P-Certificate-Subject-Common-Name From the Web GUI

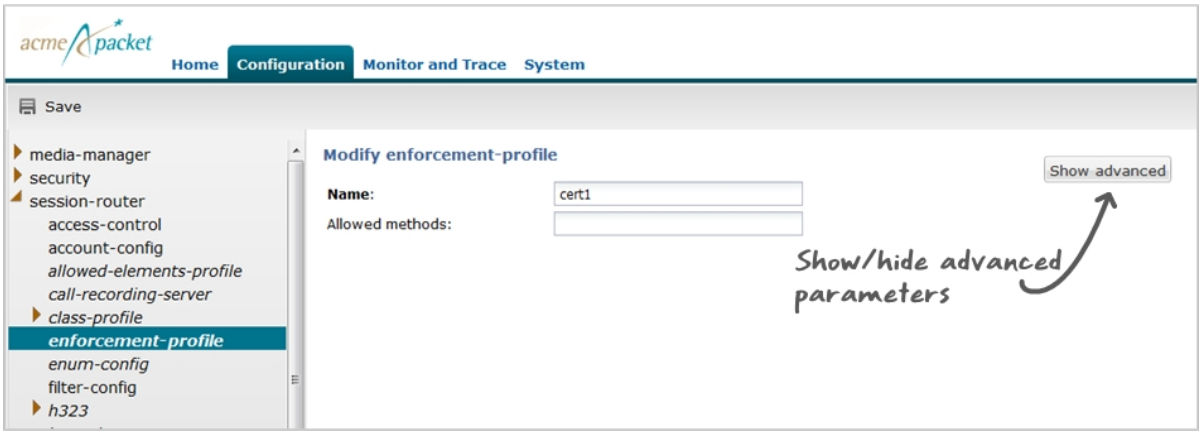
Use the following procedure to configure the P-Certificate-Subject-Common-Name using the Oracle Enterprise Session Border Controller Web GUI. In the Web GUI, this feature can be configured using Expert mode only and is an advanced configuration parameter.

To configure the P-Certificate-Subject-Common-Name in Expert mode:

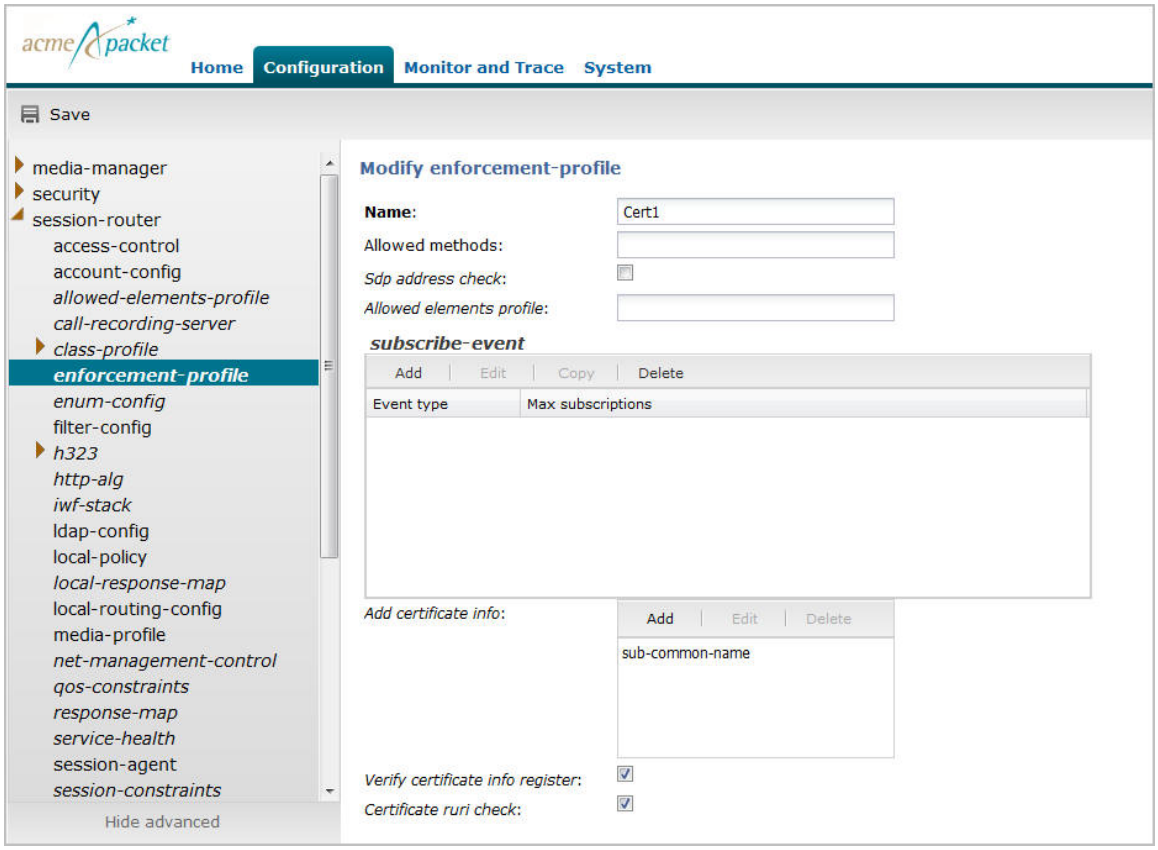
1. Logon to the Web GUI, and click Switch to Expert.
2. At the bottom of the left column, click Show advanced. The advanced elements for the objects in the left column display.



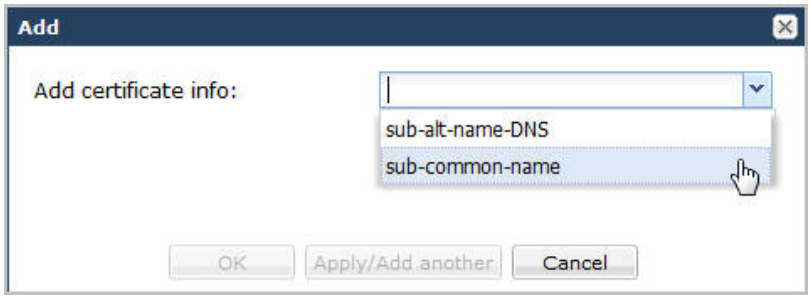
3. Click session-router.
4. Click enforcement-profile.
5. In the enforcement-profile dialog box, select the name of the certificate for which you want to enable the P-Certificate-Subject-Common-Name, and click <Edit>. The following dialog box displays.



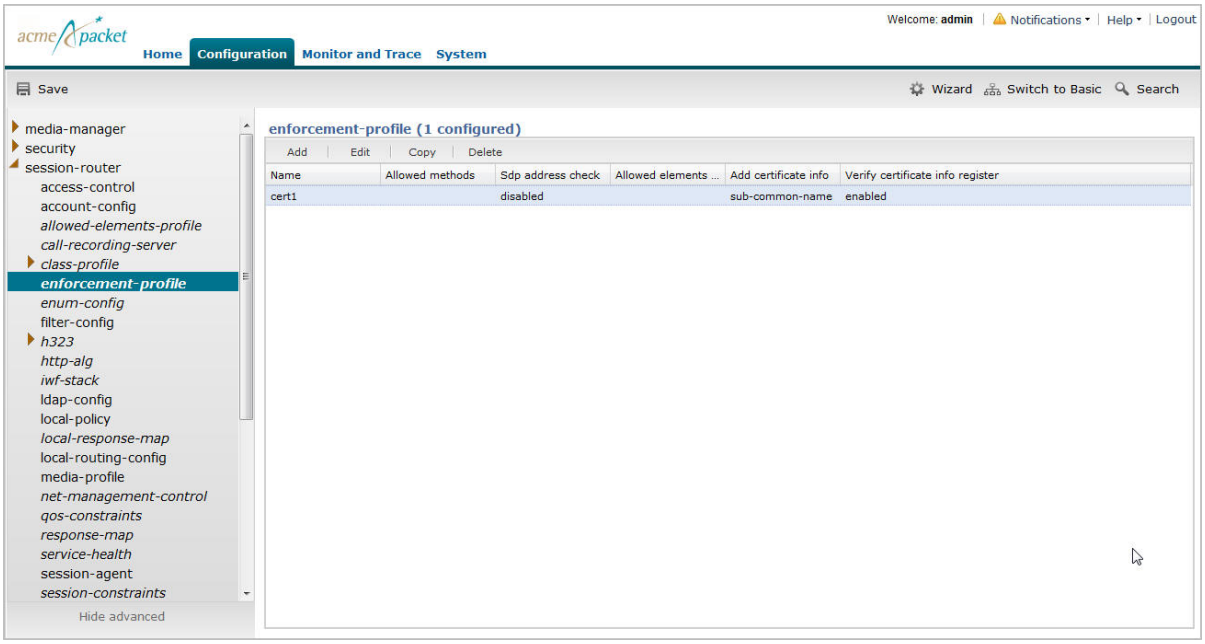
6. Click <Show advanced>. The advanced parameters for the certificate display.



7. In the Add certificate info box, click <Add>. The following dialog box displays.



8. Select sub-common-name from the drop-down box, and click <OK>.
9. In the Verify certificate info register field, place a check mark in the box to enable the Oracle Enterprise Session Border Controller to add certificate information to the header of a REGISTER message for verifying a ruri against certificate attributes. Click <OK>.
10. In the Certificate ruri check field, place a check mark in the box to enable this parameter if you want your Oracle Enterprise Session Border Controller to cache TLS certificate information and use it to validate Request-URIs. Enabling this parameter allows the Net- Net ESD to cache the TLS certificate information in a customized SIP INVITE. Click <OK>. The following window displays.



The certificate name has verify certificate info register enabled. The Oracle Enterprise Session Border Controller will include the sub-common name in the REGISTER message header before the UE registers.

SIP Monitor & Trace Enhancements

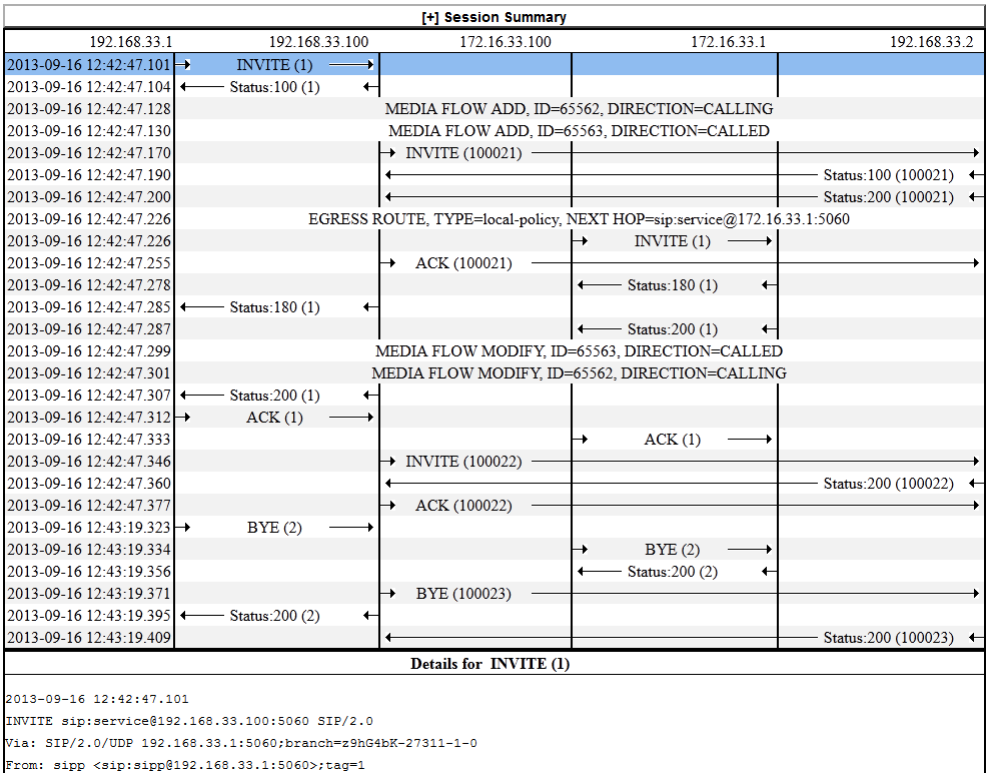
Release E-C[xz]6.4.0 M2 includes the following new feature enhancements for SIP Monitor and Trace (SM&T) in the Web GUI:

- SIPREC call data now captured and displayed in the ladder diagram in the Web GUI
- Hairpin call data now captured and displayed in the ladder diagram in the Web GUI
- SIP Monitor and Trace data now handled more efficiently on the Oracle Enterprise Session Border Controller

The following paragraphs describe these features.

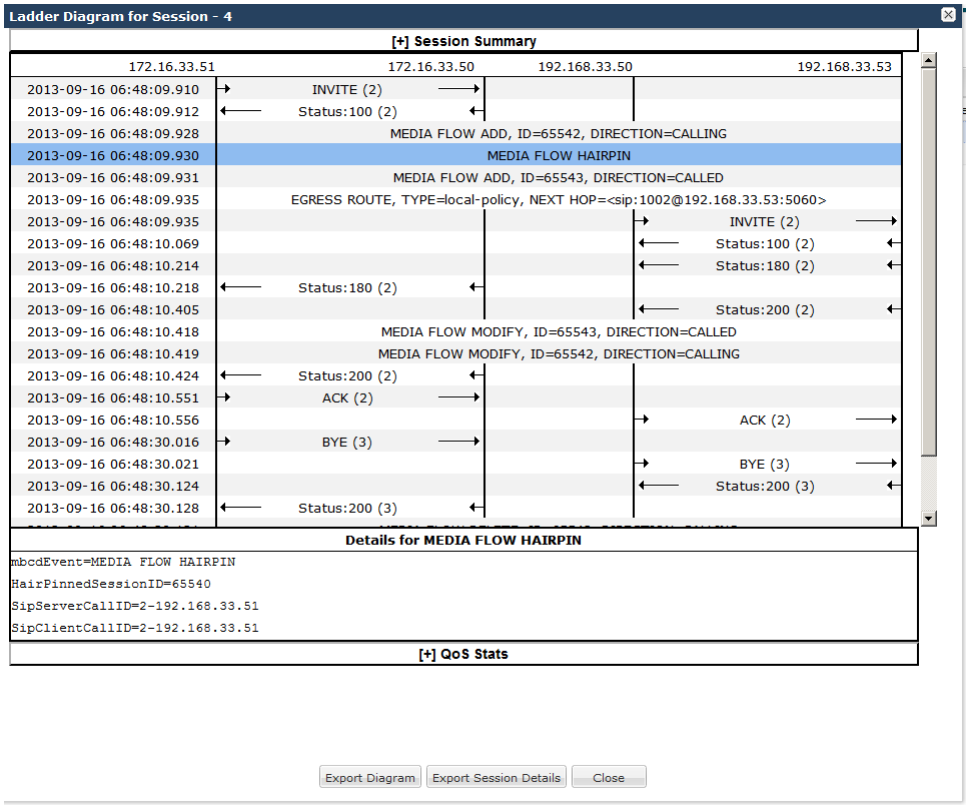
SIPREC Call Data

The following diagram shows SIP Monitor and Trace output for a call with media forwarded by way of SIPREC.



Hairpin Call Data

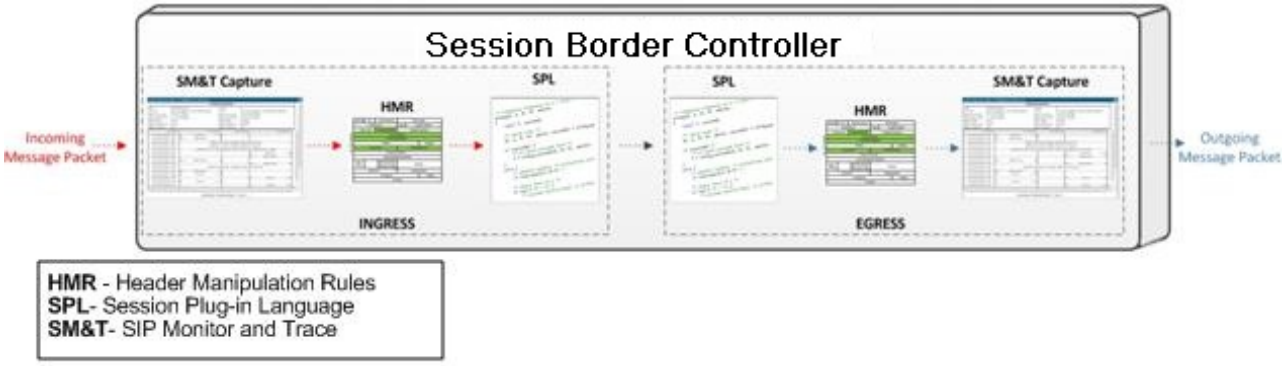
The following diagram shows SIP Monitor and Trace output for a hairpin call. Note the Media Flow Hairpin indication within the display.



SIP Monitor & Trace Ingress Egress Messages

The SM&T feature allows SIP sessions on the Oracle Enterprise Session Border Controller in your network to be monitored. Release E-C[xz]6.4.0 M2 includes a change to the way the Oracle Enterprise Session Border Controller handles SM&T data in ingress and egress messages. It processes SM&T data first on incoming messages and sends the data out last on outgoing messages. This allows the Oracle Enterprise Session Border Controller to capture SIP Monitor and Trace data over the wire for display in the Web GUI.

The Oracle Enterprise Session Border Controller captures SIP messages, applies the Header Manipulation Rules (HMR) configured on the Oracle Enterprise Session Border Controller, and then applies the Session Plug-in Language (SPL) to that message. When the message is sent out from the Net-Net ESD, it applies the SPL, then applies the HMR, and then sends out the captured SIP message.



Library Updates

Release E-C[xz]6.4.0 M2 includes the latest updates to the OpenSSL library. It also updates the SPL engine to version C2.0.2.

Licensing Information

Release E-C[xz]6.4.0 M2 removes the licensing information from the USB dongle. All licensing information can now be viewed through the Oracle Enterprise Session Border Controller Web GUI at the Help->About link, or by issuing the show about command in the ACLI.

For more information about displaying the license information, see the Net-Net Enterprise Session Director Web GUI User Guide.

Issues Resolved

The following table lists the problems resolved between Release E-C[xz]6.4.0M1 and Release E-C[xz]6.4.0M2.

Description
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for system-config->comm-monitor->local-intf in 6.4.0 GA would disappear.
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for timezone-config in 6.4.0 GA would disappear.
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for accounting-config->interim-stats-id-type in 6.4.0 GA would disappear.
After upgrading from E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, the saved configuration settings for h323-stack->alternate-transport in 6.4.0 GA would disappear.
After upgrading E-C[xz]6.4.0 GA to E-C[xz]6.4.0 M1, or downgrading from E-C[xz]6.4.0 M1 to a previous version, the saved configuration settings for session-agent->tcp-reconn-interval would disappear.

Description
In Release E-C[xz]6.4.0 GA and above, the “start-time” and “end-time” objects at the path: system->system-config->collect->group-settings, did not derive the values from the global “start time/end time”. Instead, the “start-time” always had a value of “now” and “end-time” always had a value of never for individual groups.
The system would not prevent some simultaneous ACLI and web GUI configuration sessions.
SIP traffic displayed in the SIP Monitoring and Trace Session Details was missing the Via header.
Attributes with text fields were not accepting special characters, such as quotes (" ") within the web GUI.
When a user in Basic Mode, restored an Expert Mode configuration using the System tab, an error occurred if the user then switched to the Configuration tab.
An LDAP ACL was not dynamically updating for multiple LDAP servers.
In bursty network conditions when CPU utilization was at its max, some recording sessions did not get cleaned up properly.
In certain cases modification of 'to-address' field in local policy could cause the ACLI to crash.
When running "run setup" on the ACLI and installing basic mode web configuration without a QoS license, the installation wizard was failing.
The 'use-ingress-session-params' attribute under sdes-profile and mikey-profile did not support lists.
With the sip-config option "sag-target-uri=ip" present, a DNS server status was not checked.
In some cases, the advanced configuration GUI was showing redundant entries in local-policy.
When an SDP answer was received from the unencrypted network, only one of two flows was being updated correctly. The peer-to-core flow was still left as passthrough, causing the Net-Net ESD to insert the wrong IP in the SDP answer.
In some cases, the SIP Monitor and Trace tool was showing calls as established even though the 200 OK for the BYE was never received.
An SNMP GET operation on certain OIDs would result in a leak of file descriptors, which eventually would cause an inability to check the serial number data from the USB stick (at or around midnight). The inability to read the serial number would trigger loss of licenses and failure of all calls.
An HTTP POST from Avaya phone using the Personal Profile Manager feature was failing.The problem was caused when the TCP connection on one end of a HTTP ALG session was not being terminated even though a TCP FIN was received on the other end of the HTTP ALG session.
For an H323 to SIP call, the Net-Net ESD was failing to build and send out a TCS (TerminalCapabilitySet) message to the caller when the SIP 200 OK contained an H264 codec.
PPM connections were failing when using multiple HTTP ALG entries.
The TACACS parser did not process multiple AV pairs.
The SDP sess_version was not being incremented on a Re-invite to a caller during some REFER call transfers.
In some cases, LRT DID range configurations were resulting in "invalid range entry" errors.
Sip Monitoring and Tracing did not show the Via header in outbound SIP messages.
Sip-manipulations could crash sipd in rare cases.
In some cases, neighbor table entries for gateways were not updated following a neighbor advertisement from a router when Net-Net ESD was in HA configuration.

Description
Nested regular expressions used in the processing of sip-manip rules with inmanip-before-validate option set, caused a stack overflow and subsequently a sipd task crash.
The partition mapping used on the Acme USB drive was found to be incorrect for all product releases. The filesystem allocation sizes have been corrected for the USB image used on new deployments. For existing deployments, a manual corrective action is required. Please contact TAC for additional information.
Clients were failing to connect to the SBC after reboot (the SBC was not replying to TCP "SYN" requests). This was caused by faulty ACL creation. By executing another "save" and "activate" procedure, the system successfully created the ACLs allowing the clients to connect.
SBC licenses could be lost if the VME or SE was originally installed without USB stick.
In certain "man in the middle" attacks, the HTTPS key could be exposed when accessing GUI management.
The Net-Net SD wasn't allowing two policy-attributes with the same next-hop.
Certain DNS/ENUM queries could cause a null pointer exception in SIP.
A SAG could show different destination ordering on the Web GUI than on the ACLI.

Known Issues

The following table lists Release Release E-C[xz]6.4.0 known issues and workaround steps.

Description	Workaround
Oracle Enterprise Session Border Controller Hardware	
Upon rebooting a DL320 G8 platform, a kernal crash with no restart may occur.	Do not configure VLAN on the media ports or Replace the Network Interface Card (NIC) that uses a Broadcom chip (tg3), with an Intel chip (igb), such as the HP Ethernet 1 Gb 2-port 361T Adapter (Vendor Part # 652497-B21), which is the recommended adapter.
Oracle Enterprise Session Border Controller hangs if a reboot is performed when the show support-info command is displaying results.	None
Web GUI/ACLI	
Installation wizard: If there is a hung Telnet/SSH session, you cannot perform reboot from the Virtual Machine (VM) VSphere console tab, nor can you open a new telnet session.	Reboot your VM or Oracle Enterprise Session Border Controller hardware.
When using the Web GUI, Generate Certificate and Import Certificate pop-up windows are hidden behind the Certificate Record Window	None
The SIP Monitoring and Trace Ladder diagram displays wrong Egress information when the calls are being recorded using a SIPREC server.	None
LDAP	
When configuring the “ldap-cfg-attributes” element at the path, session-router->ldap-config->ldap-transactions-	When configuring the ldap-cfg-attributes element, specify a realm to which this configuration applies. For example:

Description	Workaround
>ldap-cfg-attributes, you MUST specify a value for the realm attribute in order for calls to be received correctly.	ldap-cfg-attributes name msRTCSIP-Line next-hop sag:SA1 realm net1651 extraction-regex ^\+?1?(\d{2})(\d{3})(\d{4})$ value-format tel:+1$1$2$3
SIP KPML Interworking	
Once Key Press Markup Language (KPML)-2833 interworking is negotiated, the Oracle Enterprise Session Border Controller is not sending out a SUBSCRIBE message.	None
ACLI	
The show rec command yields no results when run on a software based SBC.	None
The show survivability command does not display stats for some SIP methods	None
The show service-health command does not display service health information if there two session agents configured with health scores greater than 100.	None

Limitations

The following table lists limitations in Release Release E-C[xz]6.4.0.

Limitation
Web Server
High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
For configurations that contain 2000 or more realms, after logging into the Web GUI and clicking on realm-config in Expert Mode, the configuration may take up to 20 seconds to load.
Hyper-V
The following are specific limitations when using Hyper-V: - Limited session capacity when using Hper-V hypervisor (50 media sessions). - Network booting is not supported due to Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors".

Limitation
- Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.

3

E-C[xz]6.4.0M3

Platform Support

The following platforms support the E-C[xz]6.4.0M3 release.

- Oracle: Net-Net 3820 and Net-Net 4500
- Server Edition: HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition: VMWare and Hyper-V

Release Image File Names

Use the following files for a new deployment.

Acme Packet Hardware

- Image: nnECX640m3.tar
- Bootloader: 01/19/2012 or newer

Server Edition. Boot Media Creator: nnECX640m3-img-usb.exe

Virtual Machines

- VMWare: nnECZ640m3-img-bin.ova
- Hyper-V: nnECZ640m3-img-bin.vhd

Upgrade Image File Names

Use the following files to upgrade a Server Edition or virtual machine deployment.

- Image: nnECZ640m3.bz
- Bootloader: nnECZ640m3.boot

Browser Support

Use the following Web browsers to access the Oracle Enterprise Session Border Controllerweb GUI.

- Windows® Internet Explorer versions 9.0 and 10.0 (version 11.0 is not supported)
- Mozilla Firefox® versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle Enterprise Session Border Controller software, clear your browser cache before using the Oracle Enterprise Session Border Controller web GUI.

Content Map

The following table lists the new features and enhancements in Release E-C[xz]6.4.0M3.

Content Type	Description
Adaptation	Configuration Inventory Widget
Adaptation	Dynamic Access Control List
Adaptation	Session Manager Mapping
Adaptation	Initial Configuration Wizard
Adaptation	Traceroute Command
Adaptation	Web GUI Search
Adaptation	Web GUI Shortcut Key Commands

New Features

Release E-C[xz]6.4.0M3 includes the following new features and enhancements.

- Configuration Inventory Control Widget
- Dynamic Access Control List
- Session Manager Mapping
- Initial Configuration Wizard
- Traceroute Command
- Web GUI Search
- Web GUI Shortcut Key Commands

Configuration Inventory Control Widget

The following table describes the new widget for the Web GUI Dashboard for Release E-C[xz]6.4.0M3.

System Widget	Description
Configuration Inventory Control	Displays a list of changes made to configuration elements. The display shows the Running Count and counts for the following types of Changes Not Activated. • Total • Added • Modified • Deleted A selectable filter can change the display from Total count to the difference between the Running Count and the Changes Not Activated Count.

Dynamic Access Control List (ACL) for the HTTP-Application Layer Gateway (ALG)

The EC[xz]6.4.0M3 release includes a dynamic ACL option for the HTTP-ALG that provides Distributed Denial of Service (DDoS) attack protection for the HTTP port.

When the dynamic ACL option is enabled, the static flow for the public listening socket defined in **http-alg > public** is created with at trust level set to **untrusted**. Each listening socket creates and manages its ACL list, which allows the listening socket to keep track of the number of received and invalid messages, the number of connections per endpoint, and so on. You can configure a different setting for each **http-alg** object.

Dynamic ACL for each endpoint is triggered by Session Initialization Protocol (SIP) registration messages. Upon receiving a SIP registration message, the SIP agent creates a dynamic ACL entry for the endpoint. If the 200 OK response is received, the ACL is promoted, allowing the HTTP message to go through the security domain. If SIP registration is unsuccessful, the ACL entry is removed and HTTP ingress messages are blocked from the endpoint. The ACL entry is removed upon incomplete registration renewal or telephone disconnect.

The following example describes the criteria and associated configuration item that result in a denied or allowed connection for both low and medium control levels.

Criteria	Associated Configuration Item	Action
Exceed total number of connections for allowed	http-alg > max-incoming-conns	Connection denied
Exceed total connections per peer	http-alg > per-src-ip-mas-incoming-conns	Connection denied
ACL not promoted	Dynamically set on SIP registration	Connection denied
Exceed maximum number of packets/sec	realm-config > maximum-signal-threshold	Connection denied and peer is demoted
Exceed maximum number of error packets	Realm-config > invalid-signal-threshold	Connection denied and peer is demoted

Oracle recommends setting **realm-config > access-control-level** to medium.

If a peer is promoted to **trusted**, the system performs DDoS checks on **max number of packets/sec** and **max number of error packets** allowed.

Demotions depend on the realm's **ream-config > access-control-trust-level** setting. For more information on **realm-config** settings, see "Personal Profile Manager (PPM) Proxy" in the "Oracle Enterprise Session Director E-C[xz]6.4.0 ACLI Configuration Guide."

If you want to configure different ACL settings for SIP traffic and for HTTP-ALG traffic, you must configure a realm for each type of traffic.

Enable Dynamic Access Control List (ACL) for the HTTP Application Layer Gateway (ALG)

Dynamic ACL option, which provides Distributed Denial of Service (DDoS) attack protection for the HTTP port, is an option that you must enable.

Confirm that the session manager is mapped to the Oracle Enterprise Session Border Controller.

Two ACL entires are required for each registered telephone, where one entry is used for SIP traffic and one is used for HTTP-ALG traffic.

Note: Enabling dynamic access control for HTTP-ALG traffic reduces the number of available dynamic ACL entries on the session border controller, which may reduce the number of concurrent trusted endpoints that the system can support.

1. From the command line, type configure terminal, and press ENTER.
2. Type session-router, and press ENTER.

3. Type http-alg, and press ENTER.
   The system displays a list of configured HTTP-ALG objects.
4. Type the number of the HTTP-ALG object that you want to edit, and press ENTER.
   The system displays the configuration values for the selected object.
5. Type dynamic-acl enabled, and press ENTER.
6. Optional. Type max-incoming-conns <value>, and press ENTER to set the maximum number of connections per peer IP address.
7. Optional. Type per-src-ip-max-incoming-conns <value>, and press ENTER to set the maximum number of HTTP connections per peer IP address.
8. Type Done, and press ENTER to save the HTTP-ALG values.
   The system displays the HTTP-ALG configuration.
9. Exit, Save, and Activate the configuration.

Dynamic Access Control List (ACL) Settings for the HTTP Application Layer Gateway (ALG)

You can set the following parameters for the realm specified in **http-alg > public > realm-id**.

- access-control-trust-level
- invalid-signal-threshold
- maximum-signal-threshold
- untrusted-signal-threshold
- deny-period

For more information on **realm-config** settings, see the ACLI Configuration Guide.

Session Manager Mapping

The E-C[xz]6.4.0M3 release supports mapping multiple session manager devices to multiple Oracle Enterprise Session Border Controller (SBC) devices. This feature allows the SBC to work in a redundant network configuration where you can map:

- The primary session manager to the primary SBC IP address
- One or more redundant session managers to one or more redundant SBCs

To map a redundant session manager to a redundant SBC, you map the private IP address of the redundant session manager to the public SIP IP address configured in HTTP-ALG > Public on the SBC. For instructions, see "Map a Session Manager to a Session Border Controller."

Map a Session Manager to a Session Border Controller

You can map one or more session managers to an Oracle Enterprise Session Border Controller (SBC) to provide redundancy and load balancing. Map the private IP address of the session manager to the public SIP interface IP address of the SBC.

Before You Begin

- Note the private IP address of the session manager and the public SIP interface IP address of the session border controller that you want to map.

Procedure

1. From the command line, type configure terminal, and press ENTER.
2. Type session-router, and press ENTER.
3. Type http-alg, and press ENTER.
   The system displays a numbered list of configured HTTP-Application Layer Gateway (ALG) objects.
4. Type the number of the HTTP-ALG object that you want to edit.
   The system displays the configuration values for the selected object.

5. Type session-manager-mapping, and press ENTER.
   The system displays a numbered list of configured HTTP-Application Layer Gateway (ALG) objects.
6. Type session-manager <IP address>, and press ENTER.
7. Type public-interface. and press ENTER.
8. Type ip-address <SBC public SIP IP address>, and press ENTER.
9. Type sip-port <port for SIP calls>, and press ENTER.
10. Type sip-transport-protocol <UDP, TCP, TLS>, and press ENTER.
11. Type done, and press ENTER.
12. Type exit, and press ENTER.
13. Type done, and press ENTER.
14. Type exit, and press ENTER.
15. Type done, and press ENTER.
16. Type show http-public-interface, and press ENTER
    The system displays the public interface values.
17. Type Done, and press ENTER to save the public interface values.
18. Exit, Save, and Activate the configuration.

Initial Configuration Wizard

Release E-C[xz]6.4.0M3 adds the Initial Configuration wizard to the Web GUI. The Initial Configuration wizard was accessible only from the command line in previous releases. You can use the Initial Configuration wizard to perform the initial configuration on an unconfigured system and to change the configuration on a configured system. During the configuration, you define the boot parameters, select the configuration mode, and select the session border controller mode. A valid license is required to run the Initial Configuration wizard.

- Unconfigured system. The system displays the Web GUI Initial Configuration wizard upon the first logon. When the initial configuration is complete, the system saves the configuration, activates the configuration, and reboots the system. The system does not backup the initial configuration of an unconfigured system.
- Configured system. Launch the Initial Configuration wizard from the Web GUI. When the re-configuration is complete, the system saves a backup of the existing configuration, saves the new configuration, activates the new configuration, and reboots the system. The backup is stored in /code/bkups.

Next Steps

- Configure the system objects.
- Optional. Reconfigure the system.

Configure the System

The system requires an initial configuration of attributes, such as modes and IP addresses, before it can function in the network.

Use the Set initial configuration wizard to define the attributes for the system. The system displays the Set initial configuration wizard upon the first logon.

Procedure

1. Logon to the Oracle Enterprise Session Border Controller.
   The system displays the Set initial configuration wizard.
2. Run the Set initial configuration wizard, and click **Complete**.
   The system saves the configuration, activates the configuration, and reboots.

Next Steps

- (Optional) Configure the system objects.

Reconfigure the System

You can reconfigure the system from the Web GUI.

Use the Set initial configuration wizard to change the initial configuration on a configured system, for example, change attributes such as IP addresses and modes.

Procedure

1. Logon to the system.
2. From the Web GUI, go to **Configuration > Wizards > Set initial configuration**.
3. Run the Set initial configuration wizard and change the attributes, as needed.
4. Click **Complete**.
   The system saves a backup of the existing configuration, saves the new configuration, activates the new configuration, and automatically reboots.

Next Steps

- (Optional) Reconfigure the system objects.

Traceroute Command

The system can trace the route of an IP packet to an Internet host by sending probe packets and listening to responses from gateways along the route. Use the traceroute command to see each host route and the round trip time of packets received from each host in a route for diagnostic purposes.

The traceroute command sends probe packets that start with a maximum time-to-live (TTL) value of one. The system listens for an Internet Control Message Protocol (ICMP) error message in response to the TTL expiry, and records the source that sent the ICMP error message. The system repeats this process and increments the TTL value by 1 for each hop in the route to the final destination.

The traceroute command returns the following information, which allows tracing the packet route to its destination.

- TTL value
- IP address of each host along the route
- Amount of time that it takes for each probe packet to travel to each host in the route

Notes:

- Unless otherwise specified, the system sends three probe packets to each host.
- The traceroute command is only available in software versions of the Oracle Enterprise Session Border Controller, for example, Server Edition (SE) and Virtual Machine Edition (VME). For more information on supported platforms, see "Platform Support."

For traceroute command syntax and arguments, see "Traceroute Command Specifications."

Examples

The following example traces the route to IP address 172.30.0.167, identifying each host in the route and the amount of time that it takes for each of three probe packets to travel to each host. The first three probe packets reach the host at 172.44.0.1 in times ranging from less than one to a little over two milliseconds. The next three probe packets reach the route destination at IP address 172.30.0.167 all in less than one millisecond.

```
ACMEPACKET# traceroute 172.30.0.167
traceroute to 172.30.0.167
1 172.44.0.1 (0.669003 ms) (2.140045 ms) (2.290964 ms)
2 172.30.0.167 (0.25602 ms) (0.219822 ms) (0.604868 ms)
```

The following example traces the route to IP address 172.30.0.167 but specifies the use of 4 probe packets instead of the default of 3.

```
ACMEPACKET traceroute 172.30.0.167 probes 4
traceroute to 172.30.0.167
1 172.44.0.1 (0.549003 ms) (1.180045 ms) (2.920584 ms) (2.48541 ms)
2 172.30.0.167 (0.25802 ms) (0.220822 ms) (0.454868 ms) (0.387574)
```

The following example specifies that the traceroute command is issued to the IP address over the user-specified network interface private and VLAN 123.

```
ACMEPACKET traceroute 10.1.2.6 intf-name:vlan private:123
traceroute to 10.1.2.6
1 10.1.2.6 (0.265121 ms) (0.599080 ms) (0.0184195 ms)
```

The following example specifies that the wait for a response timeout is 4 seconds. The default value is three seconds.

```
ACMEPACKET traceroute 10.1.2.6 timeout 4
traceroute to 10.1.2.6
1 10.1.2.6 (0.265121 ms) (0.199080 ms) (0.0284195 ms)
```

The following example specifies that the traceroute starts at a user-specified source IP address of 172.20.22.31 to a destination IP address of 10.25.2.10.

```
ACMEPACKET traceroute 172.20.22.31 source-ip 10.25.2.10
traceroute to 172.20.22.31
172.20.22.31 (0.284121 ms) (0.499770 ms) (0.084595 ms)
```

Web GUI Search

The Search function is added to the Web GUI for the Basic Configuration mode. You can search for a Basic Configuration object by name and attribute value. When you click Search, the system displays the Basic Configuration objects in a drop down list with a text box. You can select an object from the list or type an attribute in the text box. The system displays the search results in a list, where the object name is a link. Click the link to navigate to the object.

Shortcut Keys

The following tables list the shortcut key commands for the Home page and the Configuration page.

Home Page	Shortcut Key Command
Add a Widget	Ctrl+Shift+a
Refresh	Ctrl+Shift+r

Configuration Page	Shortcut Key Command
Discard	Ctrl+Shift+d
Save	Ctrl+Shift+s
Search	Ctrl+Shift+e

Known Issues

The following table describes known issues and workarounds in Release E-C[xz]6.4.0M3.

Description	Workaround
Oracle Enterprise Session Border Controller Hardware	
A newly rebooted SBC does not synchronize all data. This only affects SBCs running outside of virtual machines on non-Oracle hardware, for example, HP ProLiant DL120. When the standby SBC is rebooted, the system occasionally does not perform a full synchronization due to a timing issue during the boot sequence.	Under the **redundancy** configuration object, increase the **initial-time** value to 60000. Increasing this value changes the timing of the redundancy state change to allow the redundancy links in the SBC to come up before the application attempts synchronization.
Upon rebooting a DL320 G8 platform, a kernel crash with no restart may occur.	Do not configure VLANs on the media ports or replace the Network Interface Card (NIC) that uses a Broadcom

Description	Workaround
	chip (tg3), with an Intel chip (igb), such as the HP Ethernet 1 Gb 2-port 361T Adapter (Vendor Part # 652497-B21), which is the recommended adapter.
Oracle Enterprise Session Border Controller hangs if a reboot is performed when the show support-info command is displaying results.	None
Web GUI/ACLI	
Installation wizard: If there is a hung Telnet/SSH session, you cannot perform reboot from the Virtual Machine (VM) VSphere console tab, nor can you open a new telnet session.	Reboot your VM or Oracle Enterprise Session Border Controller hardware.
The SIP Monitoring and Trace Ladder diagram displays wrong egress information when the calls are being recorded using a SIPREC server.	None
When configuring a High Availability (HA) pair during initial configuration, the system prompts you to select "Yes" or "No" for "Acquire configuration from primary." When you select "No", the system configures both the primary instance and the secondary instance as primary instances. This configuration causes both instances to assume the active role.	Select "Yes" for "Acquire configuration from primary."
LDAP	
When configuring the “ldap-cfg-attributes” element at the path session-router->ldap-config->ldap-transactions->ldap-cfg-attributes, you MUST specify a value for the realm attribute in order for calls to be received correctly.	When configuring the ldap-cfg-attributes element, specify a realm to which this configuration applies. For example: ldap-cfg-attributes name msRTCSIP-Line next-hop sag:SA1 realm net1651 extraction-regex ^\+?1?(\d{2})(\d{3})(\d{4})$ value-format tel:+1$1$2$3
SIP KPML Interworking	
Once Key Press Markup Language (KPML)-2833 interworking is negotiated, the Oracle Enterprise Session Border Controller is not sending out a SUBSCRIBE message.	None
ACLI	
The show rec command yields no results when run on a software based SBC.	None
Upgrade	
The system does not detect a mismatch of versions when upgrading from any previous version to version M3. For example, when you upgrade from version M2P1 to	On the older version, close or refresh the browser after the upgrade to see the M3 data.

Description	Workaround
version M3, the M2 client runs on version M3 and displays only the M2 data.	

Limitations

The following table lists limitations in Release E-C[xz]6.4.0M3

Limitation
Web Server
High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
For configurations that contain 2000 or more realms, after logging into the Web GUI and clicking on realm-config in Expert Mode, the configuration may take up to 20 seconds to load.
Hyper-V
The following are specific limitations when using Hyper-V: - Limited session capacity when using Hper-V hypervisor (50 media sessions). - Network booting is not supported due to Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.
The Media Playback feature does not work on Server Edition (SE) and Virtual Machine Edition (VME).
Windows® Internet Explorer version 11 is not supported.

4

E-C[xz]6.4.0M4

Platform Support

The following platforms support the E-C[xz]6.4.0M4 release.

- Oracle: Net-Net 3820 and Net-Net 4500
- Server Edition: HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition: VMWare and Hyper-V

Release Image File Names

Use the following files for a new deployment.

Acme Packet Hardware

- Image: nnECX640m4.tar
- Bootloader: 01/19/2012 or newer

Server Edition. Boot Media Creator: nnECX640m4-img-usb.exe

Virtual Machines

- VMWare: nnECZ640m4-img-bin.ova
- Hyper-V: nnECZ640m4-img-bin.vhd

Upgrade Image File Names

Use the following files to upgrade a Server Edition or virtual machine deployment.

- Image: nnECZ640m4.bz
- Bootloader: nnECZ640m4.boot

Browser Support

Use the following Web browsers to access the Oracle Enterprise Session Border Controllerweb GUI.

- Windows® Internet Explorer versions 9.0 and 10.0 (version 11.0 is not supported)
- Mozilla Firefox® versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle Enterprise Session Border Controller software, clear your browser cache before using the Oracle Enterprise Session Border Controller web GUI.

Content Map

The following table lists the new features and enhancements in Release E-C[xz]6.4.0M4.

Content Type	Description
Adaptation	The Widgets tab, which provides users with access to individual widgets, as well as a means of creating a favorite widgets list for quick access to the users favorites.
Adaptation	The Show configuration widget displays ACLI-formatted configuration information.
Adaptation	The LRT List's Associated Config Name Column is added to the LRT configuration list for user convenience.
Adaptation	The new ACLI command, send-tcp-fin, alerts Avaya user agents to the failure of the E-SBC/Avaya Session Manager connection.
Adaptation	The new ACLI command, srtp-rekey-on-reinvite, enables E-SBC-initiated rekeying of Session Description Protocol Security Descriptions (SDES).
Adaptation	A new SPL, Attended-Transfer-Enable, provides conformity with transfer best practices as described in RFC 5589, Session Initiation Protocol (SIP) Call Control - Transfer.

New Features

Release E-C[xz]6.4.0M4 includes the following new features and enhancements.

- Graphical User Interface
  - The Widgets tab
  - The Widget tab's Favorite widgets group
  - The Show configuration Widget
  - LRT List's Associated Config name column
  - The Expert mode configuration dialog's Discard button
- Operational Features
  - TCP/FIN Send
  - SRTP Re-keying
  - Avaya Attended Transfer

Add a Widget to Favorites

The **Widgets** tab displays hierarchical lists of widgets. You can display preferred widgets under Favorites for easy access to widgets that you use often.

Procedure

1. From the Web GUI , click the Widgets tab.
2. From the All Widgets list, click the widget that you want to add to Favorites. The system displays the widget.
3. From the displayed widget, click the "Add the view to the favorites" icon. (Top, right. Shaped like a push-pin.) The system displays a success message.

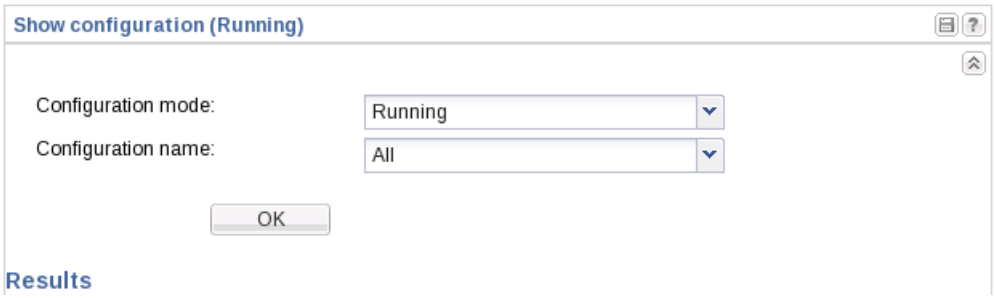
4. Click **OK**.

The Configuration Display Widget

The Oracle Enterprise Session Border Controller includes a widget that displays all or parts of either the running or editing configuration.

For those users familiar with the Oracle Enterprise Session Border Controller ACLI, examining the device's configuration from an ACLI perspective is sometimes preferable. The **Show configuration** widget can display configurations in this format.

The user specifies the output of the widget by selecting which components of the configuration they need to examine from drop-down selection list boxes and clicking OK. The widget displays the results below the settings.



Selectable **Configuration modes** include:

- Running-The currently operational configuration.
- Editing-The configuration that would become operational upon the next Activate.

In addition, the **Configuration name** drop-down allows the user to specify a subset of either the running or editing configuration to minimize the display, and focus on a specific configuration element. The user selects a single desired element from the **Configuration name** drop-down.

The LRT List's Associated Config Name Column

The Oracle Enterprise Session Border Controller Local Routing Table (LRT) configuration dialog includes column that shows the name that the device uses to refer to each LRT in the configuration.

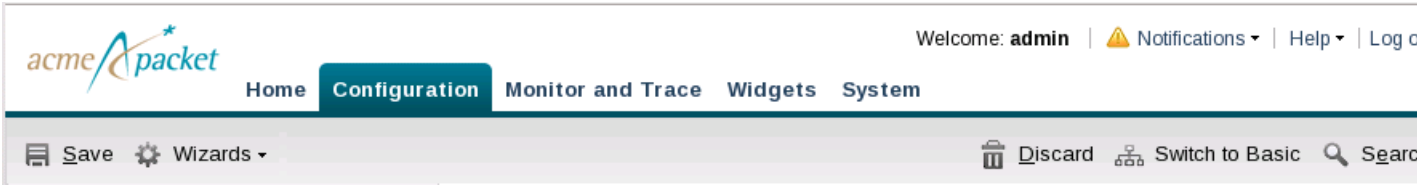
The LRT Configuration dialog displays a list of LRTs configured on the device with columns displaying important information, including:

The Association Config Name Column-An LRT's configuration name specifies the element that defines that configuration, and is used to apply that configuration elsewhere in the device configuration. This column shows that name, allowing the user to verify it has been applied correctly.

The Expert Mode Configuration Dialog's Discard Button

The Oracle Enterprise Session Border Controller's Expert mode configuration dialogs include a button that allows the user to discard configuration changes.

The **Discard** button provides the user with a means of safely backing out of configuration changes to settings that are not yet saved or activated. The button appears as a control on the right side of the configuration ribbon for all configuration dialogs.



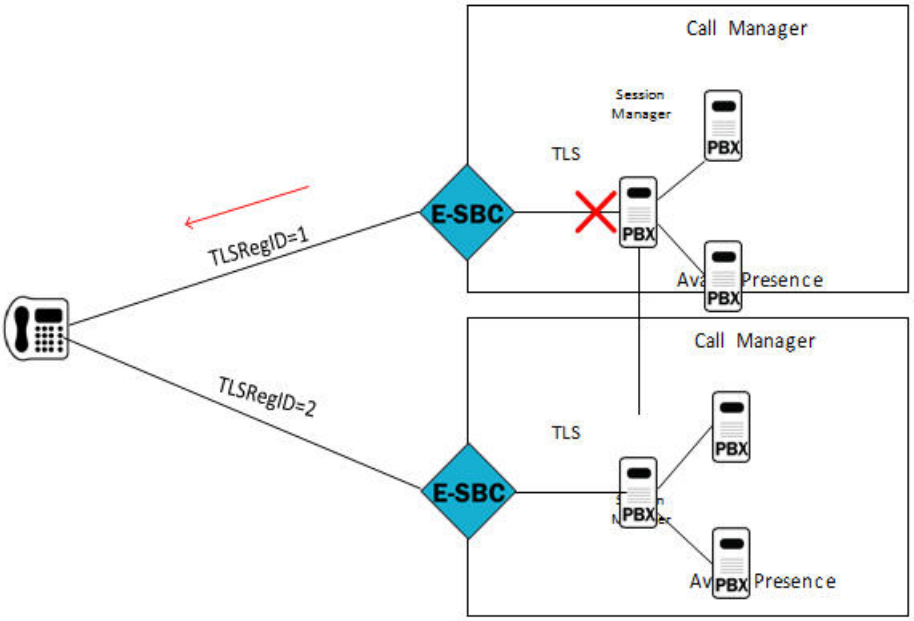
Clicking the **Discard** button causes the system to display a dialog explaining the operation and offering the user the option to cancel the discard.

Avaya Client Failover

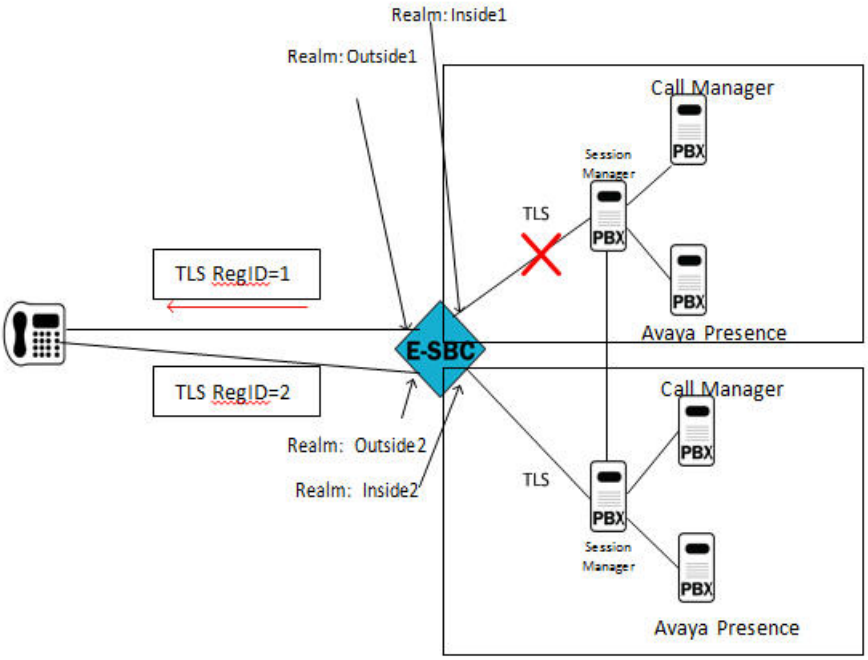
Avaya clients (telephones) require notification when the connection between the access Oracle Enterprise Session Border Controller and the Avaya Session Manager, which provides client subscription/registration services, has been lost. In the absence of such notification, the Avaya client can become unreachable for up to 24 hours. Version E-C[xy]6.4.0M4 addresses this problem by enabling anOracle Enterprise Session Border Controller that loses connectivity with an Avaya Session manager to transmit a TCP/FIN(ish) to all Avaya clients previously supported by the unreachable Session Manager. The TCP/FIN alerts clients of the need to re-register when connectivity to the Session Manager is restored.

Loss of connectivity between an Oracle Enterprise Session Border Controller and an Avaya Session Manager can result in Avaya clients (telephones) becoming unreachable for an extended period of time. Version E-C[xy]6.4.0M4 addresses this problem by enabling an E-SBC that loses connectivity with an Avaya Session manager to transmit a TCP/FIN(ish) to all Avaya clients supported by the unreachable Session Manager. The TCP/FIN alerts clients of the need to re-register when connectivity to the Session Manager is restored. In addition to issuing alerts to impacted clients, the Oracle Enterprise Session Border Controller also deletes all registrations associated with the out-of-service Session manager from the Oracle Enterprise Session Border Controller's registration cache.

A typical Avaya topology as shown below consists of a single Avaya client (a telephone), a single Oracle Enterprise Session Border Controller, and a single Avaya Session Manager, which provides subscription/registration services for the telephone. If connectivity between the Oracle Enterprise Session Border Controller and the Session Manager is lost, the Avaya client requires a TCP/FIN(ish) message that alerts the client to invalidate its subscription status, and to re-subscribe once the TCP connection becomes available. Without receipt of the TCP/FIN, the phone remains unaware of its state change, and will not receive notifies from the Session Manager until it re-subscribes, which by default is 24 hours later).



Support for redundant access topologies, based on RFC 5626, Managing Client-Initiated Connections in the Session Initiation Protocol (SIP), was introduced in Version E-C[xy]6.4.0M2. This topology accomplishes redundancy by registering an Avaya telephone to multiple Session Managers, as shown below.



In this case, the Oracle Enterprise Session Border Controller maintains connections with two Avaya Session Managers, both of which share state information and act as a registrar and proxy for the Avaya telephone. The client establishes redundancy with two TCP connections to the domain. Redundant connections are differentiated by a unique reg-id contact header field parameter. In the above illustration, two reg-ids TLSRegID 1 and TLSRegID 2 are created for different Session Managers on the same Oracle Enterprise Session Border Controller. If a Session Manager goes out-of-service, the Oracle Enterprise Session Border Controller sends a TCP/FIN message to the Avaya client for the reg-id associated with the unavailable Session Agent, and deletes all associated registration cache entries.

TCP/FIN Generation Configuration

Use the following procedure to enable a TCP/FIN exchange between the Oracle Enterprise Session Border Controller and an Avaya user agent in the event of failure of an Avaya Session Manager.

1. Access the **session-agent** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)# session-agent
ACMEPACKET(session-agent)
```

2. Select the **session-agent** object to edit.

```
ACMEPACKET(session-agent)# select
<hostname>:
1: 192.168.100.101:1813

selection: 1
ACMEPACKET(session-agent)#
```

3. **send-tcp-fin**—Set this parameter to enabled to generate a TCP/FIN exchange in response to the failure of this Avaya Session Manager. By default, this parameter is disabled.

```
ACMEPACKET(session-agent)#  send-tcp-fin enabled
ACMEPACKET(session-agent)#
```

4. Type **done** to save your configuration.
5. If necessary, repeat Steps 1 through 4 to enable TCP/FIN for other Avaya Session Managers.

SRTP Re-keying

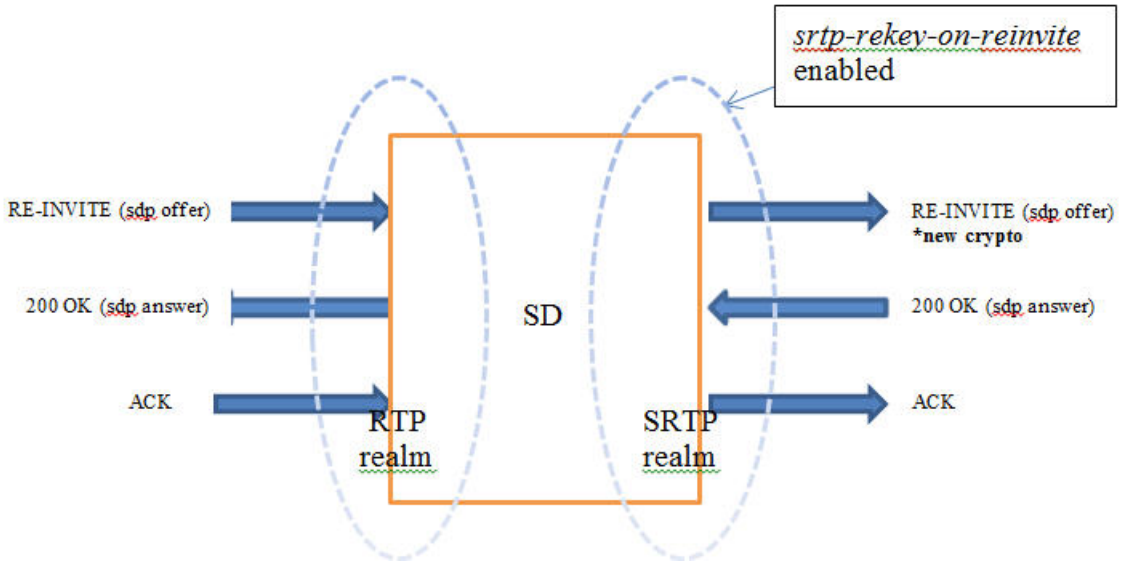
Initialization of SRTP re-keying is supported by the Oracle Enterprise Session Border Controller.

The Oracle Enterprise Session Border Controller can generate a new outbound crypto attribute in the SDP offer in a SIP re-INVITE when the **srtp-rekey-on-reinvite** parameter is set to **enabled**. The system generates the attribute regardless of the state of the flow, active or not.

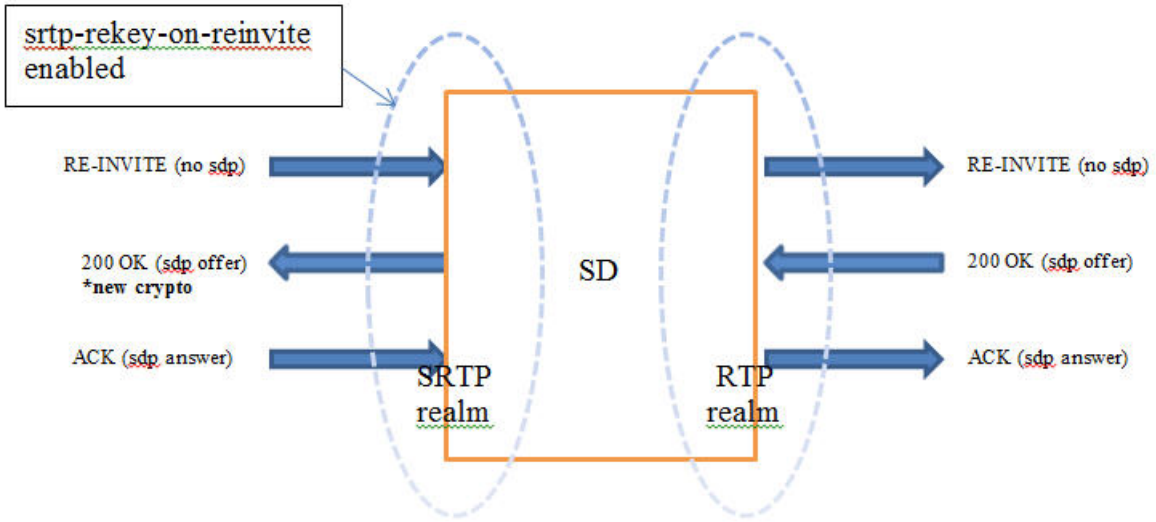
This capability is important for some clients that reside on the SRTP side in a single SRTP termination mode configuration. Any media changes that happen in the RTP side are hidden by the Oracle Enterprise Session Border Controller. This concealment may cause issues in some configurations, where media servers are involved. When the media changes from media server to called phone, the SRTP endpoint is not aware the media source changed because the SDP offer from the Oracle Enterprise Session Border Controller is the same as original invite. The result is that some devices drop packets because of Synchronization Source Identifier (SSRC) values mismatch, unexpected jumps in sequence number, sequence number reversions back to 1 triggering replay attack defense, and so forth. In certain environment is has been found that re-keying on every re-invite eliminates all these issues especially in customer setups that use Microsoft Lync products.

The processing of standard RE-INVITES (those containing an SDP offer) and offerless RE-INVITES is shown below.

With SDP:



No SDP:



If the re-invite message is a refresh and **srtp-rekey-on-reinvite** is enabled, the outbound crypto will change but the SDP version will not be incremented on the outgoing invite. If this scenario causes incompatibility issues with customer equipment then add the unique-sdp-id option to media-manager->option configuration so the Oracle Enterprise Session Border Controller increments the SDP version in the outgoing invite.

SRTP Re-keying Configuration

This procedure lists the steps required to enable SRTP re-keying.

Re-keying requires the prior configuration of an sdes-profile; this existing profile is modified to support re-keying.

An SDES profile specifies the parameter values offered or accepted during SDES negotiation. Version E-C[xy]6.4.0M4 provides a new parameter, srtp-rekey-on-reinvite, that enables the negotiation and generation of new SRTP keys upon the receipt of a SIP RE-INVITE message that contains SDP.

1. From superuser mode, use the following command sequence to access sdes-profile configuration mode.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)# sdes-profile
ACMEPACKET(sdes-profile)#
```

2. Use the select command to identify the sdes-profile to be modified
3. **srtp-rekey-on-reinvite**—Use this parameter to enable re-keying upon the receipt of an SIP RE-INVITE that contains SDP.
   - enabled—enables re-keying
   - disabled—(the default) re-keying is not supported

```
ACMEPACKET(sdes-profile)# srtp-rekey-on-reinvite enabled
ACMEPACKET(sdes-profile)#
```

4. Use done and exit to complete configuration.

Attended-Transfer-Enable SPL

Legacy Oracle Enterprise Session Border Controller software versions did not fully support the standard attended transfer scenario as it is described in RFC 5589, which describes best practices for call control and transfer of SIP-based call sessions. In a deployment in which the IP addresses on the public, or access, side of the Oracle Enterprise Session Border Controller are not routable from the private, or core, side, the flow will fail. Version E-C[xz]6.4.0M4 addresses this deficiency with a new SPL, Attended-Transfer-Enable.

Within an Avaya environment, each Avaya endpoint is known by a different URI on the access side of the Oracle Enterprise Session Border Controller than it is on the core side. Currently, when the REFER message sent from the Transferor to the Transferee crosses from the access side to the core side, the URIs in the Refer-to and Referred-by

headers are not changed from the URIs known on the access side to those known on the core side. In many cases this is easily evercome because the REFER that eventually reaches the Transferee still contains access-side URIs, which are known to the Transferee. Thus, the transferee can construct the INVITE correctly. However, in an environment in which some element of the core, such as an Avaya Session Manager (SM) or Call Manager (CM), has more control over the calls, this element may actually use the Refer-to and Referred-by URIs in its logic. For this reason, the Refer-to and Referred-by headers must contain the core-side URIs for those endpoints because the core element will have no knowledge of the access-side URIs

In order for the flow to be controlled properly, certain key URIs must be mapped from access-side to core-side and vice versa in the following messages:

- The REFER send from the Transferor to the Transfer Target
- The INVITE with Replaces header sent from the Transferee to the Transfer Target
- All subsequent requests sent from the Transferee to the Transfer Target in the dialog established by the INVITE with Replaces header

The Avaya Attended Transfer SPL provides RFC 5589 conformity by mapping access-side and core address as follows:

1. When transferor-->transfer target INVITE passes through the E-SBC from access to core, change the Refer-to URI from the access URI to the corresponding core URI.
2. When transferor-->transfer target INVITE passes through the E-SBC from access to core, change the Referred-by URI from the access URI to the corresponding core URI.
3. When transferor-->transfer target INVITE passes through the E-SBC from core to access, change the Refer-to URI from the core URI to the corresponding access URI
4. When transferor-->transfer target INVITE passes through the E-SBC from core to access, change the Referred-by URI from the core URI to the corresponding access URI.
5. When transferree-->transfer target INVITE with Replaces header passes through the SBC from access to core, change the Request-URI from the access URI to the corresponding core URI.
6. When transferree-->transfer target INVITE with Replaces header passes through the SBC from access to core, change the Referred-by URI from the access URI to the corresponding core URI.
7. When transferree-->transfer target INVITE with Replaces header passes through the SBC from core to access, change the Request-URI from the core URI to the corresponding access URI.
8. When transferree-->transfer target INVITE with Replaces header passes through the SBC from core to access, change the Referred-by URI from the core URI to the corresponding access URI
9. When any subsequent request in the dialog initiated by the INVITE with Replaces header passes through the SBC from access to core, change the Request-URI from the access URI to the corresponding core URI.
10. When any subsequent request in the dialog initiated by the INVITE with Replaces header passes through the SBC from core to access, change the Request-URI from the core URI to the corresponding access URI.

Configure the Attended-Transfer-Enable SPL

Use the following procedure to enable the Attended-Transfer-Enable SPL.

1. Access the spl-config object.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# spl-config
ACMEPACKET(spl-config)#
```

2. spl-options—Use the spl-options command to enable the Attended-Transfer-Enable SPL.

```
ACMEPACKET(system)# spl-options +attended-transfer-enable
ACMEPACKET(system)#
```

3. Use done, exit, and verify-config to complete the configuration.
4. Activate the new configuration.

Known Issues

The following table describes known issues and workarounds in Release E-C[xz]6.4.0M4.

Description	Workaround
Oracle Enterprise Session Border Controller Hardware	
A newly rebooted SBC does not synchronize all data. This only affects SBCs running outside of virtual machines on non-Oracle hardware, for example, HP ProLiant DL120. When the standby SBC is rebooted, the system occasionally does not perform a full synchronization due to a timing issue during the boot sequence.	Under the **redundancy** configuration object, increase the **initial-time** value to 60000. Increasing this value changes the timing of the redundancy state change to allow the redundancy links in the SBC to come up before the application attempts synchronization.
Upon rebooting a DL320 G8 platform, a kernel crash with no restart may occur.	Do not configure VLANs on the media ports or replace the Network Interface Card (NIC) that uses a Broadcom chip (tg3), with an Intel chip (igb), such as the HP Ethernet 1 Gb 2-port 361T Adapter (Vendor Part # 652497-B21), which is the recommended adapter.
Oracle Enterprise Session Border Controller hangs if a reboot is performed when the show support-info command is displaying results.	None
Web GUI/ACLI	
Installation wizard: If there is a hung Telnet/SSH session, you cannot perform reboot from the Virtual Machine (VM) VSphere console tab, nor can you open a new telnet session.	Reboot your VM or Oracle Enterprise Session Border Controller hardware.
The SIP Monitoring and Trace Ladder diagram displays wrong egress information when the calls are being recorded using a SIPREC server.	None
When configuring a High Availability (HA) pair during initial configuration, the system prompts you to select "Yes" or "No" for "Acquire configuration from primary." When you select "No", the system configures both the primary instance and the secondary instance as primary instances. This configuration causes both instances to assume the active role.	Select "Yes" for "Acquire configuration from primary."
LDAP	
When configuring the “ldap-cfg-attributes” element at the path session-router->ldap-config->ldap-transactions->ldap-cfg-attributes, you MUST specify a value for the realm attribute in order for calls to be received correctly.	When configuring the ldap-cfg-attributes element, specify a realm to which this configuration applies. For example: ldap-cfg-attributes name msRTCSIP-Line next-hop sag:SA1 realm net1651 extraction-regex ^\+?1?(\d{2})(\d{3})(\d{4})$ value-format tel:+1$1$2$3

Description	Workaround
SIP KPML Interworking	
Once Key Press Markup Language (KPML)-2833 interworking is negotiated, the Oracle Enterprise Session Border Controller is not sending out a SUBSCRIBE message.	None
ACLI	
The show rec command yields no results when run on a software based SBC.	This issue is resolved in the M4 release.
Upgrade	
The system does not detect a mismatch of versions when upgrading from any previous version to version M3. For example, when you upgrade from version M2P1 to version M3, the M2 client runs on version M3 and displays only the M2 data.	This issue is resolved in the M4 release.

Limitations

The following table lists limitations in Release E-C[xz]6.4.0M4.

Limitations
Web Server
High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
For configurations that contain 2000 or more realms, after logging into the Web GUI and clicking on realm-config in Expert Mode, the configuration may take up to 20 seconds to load.
Hyper-V
The following are specific limitations when using Hyper-V: - Limited session capacity when using Hyper-V hypervisor (50 media sessions). - Network booting is not supported due to Microsoft Firewall Test (MSFT) driver defect. - Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.
The Media Playback feature does not work on Server Edition (SE) and Virtual Machine Edition (VME).
Windows® Internet Explorer version 11 is not supported.

5

E-C[xz]6.4.0M5

Oracle Enterprise Session Border Controller Description

The Oracle Enterprise Session Border Controller (E-SBC) connects disparate Internet Protocol (IP) communications networks while mitigating security threats, curing interoperability problems, and ensuring reliable communications. The E-SBC protects and controls real-time voice, video, and Unified Communications (UC) as they traverse IP network borders.

Overview

Available in software and appliance configurations, the E-SBC is highly scalable and includes an industry-leading feature set.

- Strong security. As the E-SBC protects IP telephony and UC infrastructure, services, and applications, it also ensures confidentiality, integrity, and availability. The E-SBC protects against fraud, service theft, malicious attacks, system overloads, and other events that affect service.
- Easy interoperability. The E-SBC provides extensive signaling and media control features to help businesses overcome interoperability challenges that commonly occur when interfacing with public IP network services. The E-SBC also performs protocol interworking and dial plan management for integration with legacy systems.
- Assured reliability. The E-SBC ensures Public Switched Telephone Networks (PSTN)-like availability and service quality for IP communications. The E-SBC enforces service quality, balances loads across trunks, and reroutes sessions around interface disruptions to optimize network performance, circumvents equipment and facility problems, and ensures business continuity.

Functions and Modes

Businesses install the E-SBC at Session Initiation Protocol (SIP) network borders, where enterprise communications systems interface with public network services and where disparate multi-vendor systems must be managed.

Customers use the E-SBC to:

- Connect to SIP trunking services and the Internet
- Access communications services
- Communicate securely with remote workers
- Manage sessions across a multi-vendor UC environment
- Connect contact center locations and Business Process Outsourcing (BPO) services

Platform Support

The following platforms support the E-C[xz]6.4.0M5 release.

- Oracle: Net-Net 3820 and Net-Net 4500
- Server Edition: HP DL120 G7, HP DL320e G8, and Dell R210 II
- Virtual Machine Edition: VMWare and Hyper-V

Release Image File Names

Use the following files for a new deployment.

Acme Packet Hardware

- Image: nnECX640m5.tar
- Bootloader: 01/19/2012 or newer

Server Edition

- Boot Media Creator: nnECZ640m5-img-usb.exe

Virtual Machine

- VMWare: nnECZ640m5-img-bin.ova
- Hyper-V: nnECZ640m5-img-bin.vhd

Upgrade Image File Names

Use the following files to upgrade a Server Edition or virtual machine deployment.

- Image: nnECZ640m5.bz
- Bootloader: nnECZ640m5.boot

Browser Support

Use the following Web browsers to access the Oracle Enterprise Session Border Controller Web GUI.

- Windows® Internet Explorer versions 9.0 and 10.0 (version 11.0 is not supported)
- Mozilla Firefox® versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher

Note: After upgrading your Oracle Enterprise Session Border Controller software, clear your browser cache before using the Oracle Enterprise Session Border Controller Web GUI.

Content Map

The following table lists the new features and enhancements in release E-C[xz]6.4.0M5.

Content Type	Description
Adaptation	Administrative Security ACP License
Adaptation	SIP hold-refer-reinvite Option

New Features

The baseline for the EC[xz]6.4.0M5 release is the EC[xz]6.4.0M4 release.

The E-C[xz]6.4.0M5 release includes the following new features and enhancements.

- Administrative Security ACP License
- SIP hold-refer-reinvite Option

Administrative Security ACP License

The Administrative Security ACP license adds more password security and opens the ACP port for remote configuration.

The Administrative Security ACP license inherits the rules of the Administrative Security license and imposes additional rules and restrictions to improve password strength. For example, the Administrative Security ACP license overrides the minimum character length rules for passwords that are defined in the Administrative Security license and enforces stronger rules. The system does not require the presence of both licenses because the Administrative Security license is not a prerequisite for the Administrative Security ACP license. Either license can stand alone. The system supports the presence of both licenses, for example, in a deployment where the Administrative Security ACP license is added to a system with an active Administrative Security license.

The following scenarios describe system behavior with and without the presence of the Administrative Security license and the Administrative Security ACP license.

- Scenario: The Administrative Security license and the Administrative Security ACP license are both deployed and you enable password-policy-strength.

  Behavior: The Administrative Security ACP license defines the password rules and opens the ACP port.

- Scenario: The Administrative Security license and the Administrative Security ACP license are both deployed and you disable password-policy-strength.

  Behavior: The Administrative Security license defines the password rules and the ACP port remains open.

- Scenario: The Administrative Security ACP license is deployed alone and you disable password-policy-strength.

  Behavior: The system enforces the underlying Admin Security license password rules, which are less strict, and keeps the ACP port open.

- Scenario: The Administrative Security license is deployed alone.

  Behavior: The Administrative Security license defines the password rules and the system closes the ACP port.

- Scenario: Neither the Administrative Security license nor the Administrative Security ACP license is deployed.

  Behavior: The system enforces no password rules and keeps the ACP port open.

When enabled, the Administrative Security ACP license applies the following rules and restrictions to passwords for all local users to ensure that their passwords are not easily guessed.

- Minimum of 9 characters required for a user-level password
- Minimum of 15 characters required for an admin-level password
- Must contain at least 2 upper case letters
- Must contain at least 2 lower case letters
- Must contain at least 2 numerical characters
- Must contain at least 2 special characters
- May not contain, repeat, or reverse the associated user ID
- May not contain two or more characters from the user ID. For example, if the user ID is "admin" and the password is "migda", the system rejects the password because "mi" appears in both words.
- May not use the same character more than 3 times, consecutively
- May not contain a sequence of three or more characters from a previous password. For example, if the existing password is "3birds", the new password cannot include '3bi', 'bir', 'ird', and so on.
- May not contain a sequence of two or more characters more than once. For Example, w29c29 is not allowed.
- May not contain sequential numbers or characters or a repeated character or number. For example, '66666', 'aaaa', 'abcd', 'fedc', '1234', '7654'.

- Must differ by at least four characters from the previous password
- May not use NULL password

Note: The Administrative Security ACP license does not support SSH user names and SSH passwords that are stored locally, and this license does not support RADIUS users.

For more information, see "Administrative Security ACP License Configuration" and "Enable the Administrative Security ACP License."

Administrative Security ACP License Configuration

You must enable the Administrative Security ACP license to enforce the stronger password restrictions that it provides.

You cannot change the password configuration rules and restrictions that the Administrative Security ACP license imposes, but you can enable or disable this license to apply or ignore the rules and restrictions.

From the ACLI, use the password-policy-strength command under the password-policy configuration element to enable or disable the Administrative Security ACP license and to specify the password change policy rules.

Note: The ACP port remains open whether the password-policy-strength command is enabled or disabled.

The password-policy configuration element displays the min-secure-pwd-len command. You do not need to configure the min-secure-pwd-len command when you enable the Administrative Security ACP license because this license overrides this command with a stronger rule.

The password-policy configuration element displays the following password policy commands that you can configure.

- expiry-interval. Specifies the password lifetime in days. Password lifetime tracking begins when a password is changed. The range is 1-65535 days.
- expiry-notify-period. Specifies the number of days prior to expiration when the system starts sending password expiration notifications. The range is 1-90 days.
- grace-period. Specifies the number of days that the system allows for grace log on attempts after password expiration. The range is 1-90 days.
- grace-logins. Specifies the number of log on attempts that the system allows during the grace period. The range is 1-10 attempts.
- password-history-count. Specifies the number of previously used passwords retained in the password history cache. The range is 1-10 passwords.
- password-change-interval. Specifies the minimum time that must elapse between password changes. A user cannot change a password more than once every password change interval. The range is 1-24 hours.

For enablement and configuration instructions, see "Enable the Administrative Security ACP License."

Enable the Administrative Security ACP License Password Rules

To enforce the stronger password rules and restrictions that the Administrative Security ACP license it provides, you must enable the password-policy-strength parameter.

- Confirm that the Administrative Security ACP license is installed on the system.
- You must have Superuser permissions.

From the command line, go to the password-policy configuration element and set the password-policy-strength parameter to enabled.

Note: The password-policy configuration element displays the min-secure-pwd-len command. You do not need to configure the min-secure-pwd-len command because the Administrative Security ACP license overrides this command with a stronger rule.

You can configure any of the other password policy settings without a system override, according to the ranges specified in this procedure. For more information about the ranges, see "Administrative Security ACP License Configuration."

1. Access the **password-policy** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# password-policy
ACMEPACKET(password-policy)#
```

2. Type select, and press ENTER.
3. Type show, and press ENTER.
4. Configure the following password policy settings, as needed:
   - expiry-interval. 1-65535 days.
   - expiry-notify-period. 1-90 days.
   - grace-period. 1-90 days.
   - grace-logins. 1-10 attempts.
   - password-history-count. 1-10 passwords.
   - password-change-interval. 1-24 hours.
   - password-policy-strength. Type enabled, and press ENTER.
5. Do the following:
   1. Type done, and press ENTER.
   2. Type exit, and press ENTER.
   3. Type done, and press ENTER.

Password Expiry for the Administrative Security ACP License

The system ages passwords and requires the user to change the password after the specified time interval.

The password change interval is configurable by way of the expiry-interval command. The range is from 0-65535 days. The default interval is 90 days

Password lifetime tracking begins when a password is changed. The system sends a notification to the user during log on and log off, when the password nears expiration. Use the expiry-notify-period command to configure the number of days in advance of password expiry that the system sends the notification. The range from 1-90 days. The default is 30 days.

The system can continue to accept log on attempts after the password expiration grace period, according to the following rules:

- Grace logins. The number of login attempts that the system allows during the grace period. The range is 1-10 attempts.
- Grace period. The number of days that the system allows for grace logins after password expiration. The range is 1-90 days.

When either the grace period expires or the number of grace logins is reached, the system forces the user to change the password.

The system maintains a history of passwords by storing up to 10 previous passwords. When the password is changed, the system adds the most recent password to the history and deletes the oldest password from the history. Every time the password is changed, the system compares the new password to the password history. A new password must differ from every password in the history.

For configuration instructions, see "Enable the Administrative Security ACP License."

SIP hold-refer-reinvite

When SIP hold-refer-reinvite is enabled for REFER with Replaces, the system queues the outgoing Invite populated from the received REFER based on the dialog state.

In a deployment where a call goes through the Oracle Enterprise Session Border Controller (E-SBC) before going to an Interactive Voice Response (IVR) server, the E-SBC proxies the intermediate reinvite that the IVR sends to the transfer target. If the intermediate reinvite is in either the pending state or the established state when the IVR initiates the transfer to the transfer target, the E-SBC terminates the call prematurely. The hold-refer-reinvite option allows the

E-SBC to queue the Out Going INVITE from the received REFER request when the previously proxied reinvite request is in either the pending state or the established state. The result is a successful call.

Enable the SIP hold-refer-reinvite option from the ACLI command line or the Web GUI in Expert mode.

Enable hold-refer-reinvite - ACLI

The SIP hold-refer-reinvite parameter for REFER with Replaces is a parameter that you enable to prevent premature call termination in a deployment where calls are proxied by the Oracle Enterprise Session Border Controller.

- Confirm that refer-reinvite is added to realm/SA/SipInterface options.
- Confirm that refer-call-transfer is enabled on realm/SA/SipInterface
- Confirm that the session agent on which you want to enable hold-refer-reinvite is configured.

To enable hold-refer-reinvite, select a configured session agent and enable the parameter on the selected agent.

1. Access the **session-agent** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)# session-agent
ACMEPACKET(session-agent)
```

2. Type select, and press ENTER.
   The system displays a numbered list of session-agents.
3. Type the number of the agent on which you want to enable hold-refer-invite, and press ENTER.
4. Type hold-refer-reinvite enabled, and press ENTER.
5. Type done to save the configuration.

- Enable the refer-hold-reinvite parameter in the realm configuration.
- Enable the refer-hold-reinvite parameter in the session agent configuration.

Known Issues

The following table describes known issues and workarounds in release E-C[xz]6.4.0M5.

Description	Workaround
Oracle Enterprise Session Border Controller Hardware	
A newly rebooted SBC does not synchronize all data. This only affects SBCs running outside of virtual machines on non-Oracle hardware, for example, HP ProLiant DL120. When the standby SBC is rebooted, the system occasionally does not perform a full synchronization due to a timing issue during the boot sequence.	Under the **redundancy** configuration object, increase the **initial-time** value to 60000. Increasing this value changes the timing of the redundancy state change to allow the redundancy links in the SBC to come up before the application attempts synchronization.
Upon rebooting a DL320 G8 platform, a kernel crash with no restart may occur.	Do not configure VLANs on the media ports or replace the Network Interface Card (NIC) that uses a Broadcom chip (tg3), with an Intel chip (igb), such as the HP Ethernet 1 Gb 2-port 361T Adapter (Vendor Part # 652497-B21), which is the recommended adapter.
Oracle Enterprise Session Border Controller hangs if a reboot is performed when the show support-info command is displaying results.	None
Web GUI and ACLI	
Installation wizard: If there is a hung Telnet/SSH session, you cannot perform reboot from the Virtual	Reboot your VM or Oracle Enterprise Session Border Controller hardware.

Description	Workaround
Machine (VM) VSphere console tab, nor can you open a new telnet session.	
The SIP Monitoring and Trace Ladder diagram displays wrong egress information when the calls are being recorded using a SIPREC server.	None
When configuring a High Availability (HA) pair during initial configuration, the system prompts you to select "Yes" or "No" for "Acquire configuration from primary." When you select "No", the system configures both the primary instance and the secondary instance as primary instances. This configuration causes both instances to assume the active role.	Select "Yes" for "Acquire configuration from primary."
LDAP	
When configuring the “ldap-cfg-attributes” element at the path session-router->ldap-config->ldap-transactions->ldap-cfg-attributes, you MUST specify a value for the realm attribute in order for calls to be received correctly.	When configuring the ldap-cfg-attributes element, specify a realm to which this configuration applies. For example: ldap-cfg-attributes name msRTCSIP-Line next-hop sag:SA1 realm net1651 extraction-regex ^\+?1?(\d{2})(\d{3})(\d{4})$ value-format tel:+1$1$2$3
SIP KPML Interworking	
Once Key Press Markup Language (KPML)-2833 interworking is negotiated, the Oracle Enterprise Session Border Controller is not sending out a SUBSCRIBE message.	None

Limitations

The following table lists limitations in release E-C[xz]6.4.0M5.

Limitations
Web Server
High-frequency logging into and out of the GUI using an automation script (a rate faster than humanly possible) results in a system crash. It is not expected that manual testing will produce this issue.
For configurations that contain 2000 or more realms, after logging into the Web GUI and clicking on realm-config in Expert Mode, the configuration may take up to 20 seconds to load.
Hyper-V
The following are specific limitations when using Hyper-V: - Limited session capacity when using Hyper-V hypervisor (50 media sessions). - Network booting is not supported due to Microsoft Firewall Test (MSFT) driver defect.

Limitations
- Dynamic Host Configuration Protocol (DHCP) is not supported due to the MSFT driver defect. - Microsoft does not support USB pass-through via hypervisor. - Virtual LAN (VLAN) tagging is not supported with Hyper-V in Windows 2008 R2. - When using High Availability (HA), the wancom interfaces should be configured as "Legacy Network Adaptors". - Microsoft System Center Virtual Machine Manager (MS-SCVMM) should not be used to deploy Oracle Virtual Machine Edition (VME) products due to a Virtual Hard Disk (VHD) import defect.
The Media Playback feature does not work on Server Edition (SE) and Virtual Machine Edition (VME).
The system does not support using the Media Playback feature in conjunction with the SIPREC feature.
Windows® Internet Explorer version 11 is not supported.